ROD

mały kodeks postępowania dla agencji zatrudnienia

II EDYCJA 2021

RODO

mały kodeks postępowania dla agencji zatrudnienia

II EDYCJA 2021

Polskie Forum HR

Redakcja:

r. pr. Liliana Strupp

Autorzy opracowania:

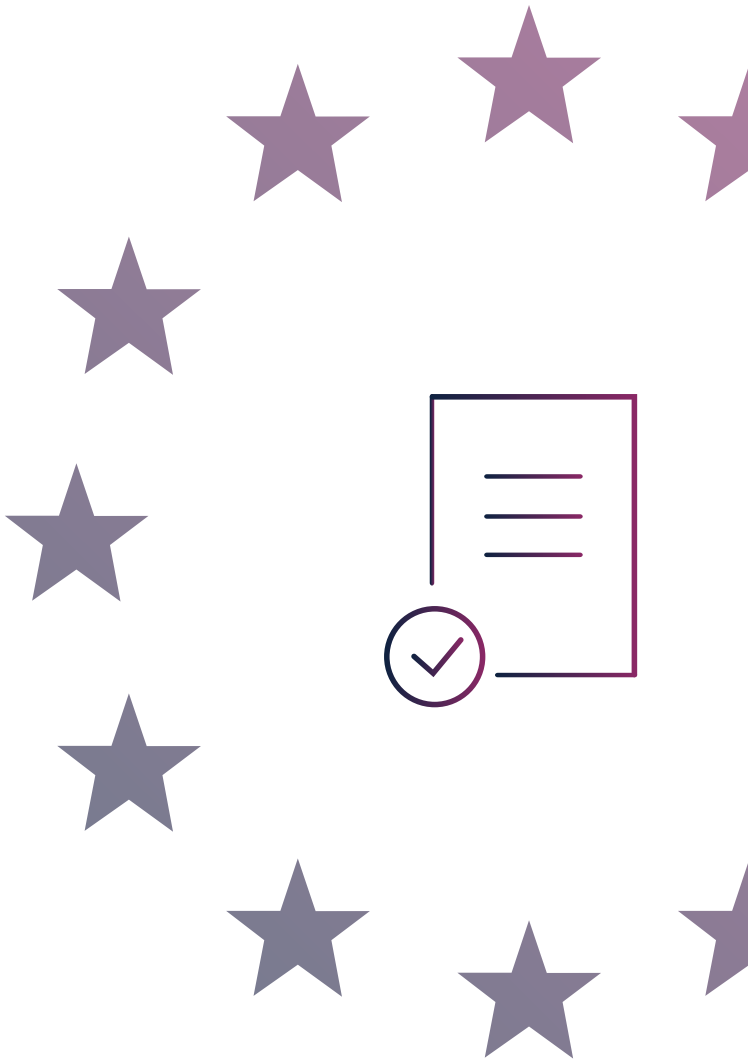
Małgorzata Brańska, CISA, CIPP/E
r. pr. Dominika Domiańska-Drzazga
Przemysław Frańczak
r. pr. Olga Gierada-Jabłonka
apl. adw. Karolina Kot
Anna Prokulska
apl. adw. Marzena Przeworska
r. pr. Piotr Stolarczyk
r. pr. Liliana Strupp

Pierwsza edycja: RODO mały kodeks postępowania, 2018, redakcja: r. pr. Liliana Strupp, autorzy opracowania:
Barbara Drabich, Paweł Olejniczak, r. pr. Małgorzata Sitkiewicz, r. pr. Piotr Stolarczyk, r. pr. Liliana Strupp, r. pr. dr Małgorzata Wilińska

SPIS TREŚCI

WSTĘP

Wprowadzając Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z 27.04.2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych) – dalej „RODO", europejski prawodawca stworzył przepisy o charakterze generalnym i neutralnym, tak aby nieustający postęp techniczny, technologiczny i informatyczny nie stwarzał konieczności ciągłego ich dostosowywania do zmieniającego się otoczenia. Dlatego też RODO nie wskazuje wprost ani nie rekomenduje żadnych środków technicznych, czy organizacyjnych (z kilkoma wyjątkami), które miałyby być obowiązkowo stosowane przez organizacje w procesach przetwarzania danych osobowych. RODO wskazuje jedynie kilka ogólnych zasad, którymi należy kierować się przy projektowaniu rozwiązań biznesowych i informatycznych.



Główne idee RODO

1

GŁÓWNE IDEE RODO

Głównym przesłaniem towarzyszącym przygotowaniu i wprowadzeniu w życie RODO było ułatwienie przepływu danych osobowych poprzez jego uregulowanie. Całość podejścia do ochrony danych osobowych opiera się na ryzyku, a samo słowo „ryzyko" pojawia się w RODO kilkadziesiąt razy. Każdy przedsiębiorca powinien sam określić ryzyka, jakie mogą być obecne w codziennym przetwarzaniu danych osobowych i na tej podstawie opracować i wdrożyć odpowiednie zabezpieczenia techniczne i organizacyjne.

RODO wprowadza pojęcia „ochrony danych w fazie projektowania" (*privacy by design*) i „domyślnej ochrony danych" (*privacy by default*). Oznacza to, że już podczas planowania procesów i systemów, w których będą przetwarzane dane osobowe, należy zadbać o zabezpieczenia adekwatne do ryzyk oraz do celu, zakresu i kontekstu przetwarzanych danych. Domyślna ochrona danych to nic innego, jak gromadzenie tylko tych danych, które są niezbędne do realizacji procesu biznesowego i przetwarzanie ich tylko przez taki czas, jaki jest potrzebny do realizacji tych celów.

Najważniejsze pojęcia

2

NAJWAŻNIEJSZE POJĘCIA

Agencja
Agencja zatrudnienia lub agencja pracy tymczasowej w rozumieniu Ustawy z 20.04.2004 r. o promocji zatrudnienia i instytucjach rynku pracy (Dz.U. z 2019 r. poz. 1482) – dalej „Ustawa o promocji zatrudnienia".

Dane osobowe
Dane identyfikujące lub pozwalające zidentyfikować osobę fizyczną, np. imię i nazwisko, PESEL, adres e-mail, numer telefonu, rozmiar obuwia i odzieży roboczej, składniki pensji, wymiar urlopu, wykształcenie, doświadczenie zawodowe kandydata, fotografia, kadr z monitoringu, adres IP.

Dane wrażliwe | Inaczej: *dane sensytywne*
Dane osobowe ujawniające pochodzenie rasowe lub etniczne, poglądy polityczne, przekonania religijne lub światopoglądowe, przynależność do związków zawodowych oraz przetwarzania danych genetycznych, danych biometrycznych w celu jednoznacznego zidentyfikowania osoby fizycznej lub danych dotyczących zdrowia, seksualności lub orientacji seksualnej tej osoby.

Dane biometryczne
Informacje pozwalające zidentyfikować osobę na podstawie jej unikalnych cech biologicznych, poprzez porównanie zapisu tych cech z bazy danych z nową próbką i określenie, czy są identyczne. Wynikają z przetwarzania zautomatyzowanego, dotyczą cech fizycznych, fizjologicznych lub behawioralnych osoby fizycznej oraz umożliwiają lub potwierdzają jednoznaczną identyfikację tej osoby, np. odcisk palca, odcisk kształtu dłoni, obraz tęczówki oka.

Dane dotyczące zdrowia
Dane osobowe o zdrowiu fizycznym lub psychicznym osoby fizycznej, w tym o korzystaniu z usług opieki zdrowotnej, ujawniające informacje o przeszłym, obecnym lub przyszłym stanie zdrowia fizycznego lub psychicznego, np. stopień niepełnosprawności, wyniki badań, konieczność noszenia okularów korekcyjnych do pracy z komputerem, informacja o ciąży, fakt odbywania terapii, czy zawartość alkoholu we krwi.

Osoba, której dane dotyczą | Inaczej: *Podmiot danych*
Osoba, do której odnoszą się dane osobowe, np.

kandydat do pracy, pracownik, pracownik tymczasowy, członkowie rodziny pracownika, przedstawiciel dostawcy, reprezentant klienta.

Zgoda
Dobrowolne, konkretne, świadome i jednoznaczne okazanie woli osoby, której dane dotyczą, w formie oświadczenia lub wyraźnego działania potwierdzającego, przyzwalające na przetwarzanie dotyczących jej danych osobowych, np. kliknięcie przycisku „wyrażam zgodę", zaznaczenie kratki ze zgodą w aplikacji, przesłanie listem czy podpis na formularzu.

Przetwarzanie danych osobowych
Każde działanie wykonywane na danych osobowych, w szczególności: zbieranie, utrwalanie, udostępnianie, przechowywanie, modyfikowanie, pobieranie, wykorzystywanie, usuwanie, niszczenie, przeglądanie, ograniczanie, a także czytanie, czyli wgląd do danych.

Transgraniczne przetwarzanie danych
Transgraniczne przetwarzanie danych ma miejsce, gdy organizacja ma swoje jednostki w więcej niż jednym kraju członkowskim Unii Europejskiej (UE), a także wtedy, gdy organizacja mająca siedzibę w jednym z krajów UE przetwarza dane osób z różnych krajów UE.

Państwo trzecie
Państwo nienależące do Europejskiego Obszaru Gospodarczego (EOG), który obejmuje kraje Unii Europejskiej oraz Islandię, Norwegię i Liechtenstein. Państwem trzecim w rozumieniu RODO jest np. Ukraina, Szwajcaria czy Stany Zjednoczone.

Administrator danych osobowych
Podmiot, który samodzielnie lub wspólnie z innymi podmiotami ustala cele i sposoby przetwarzania danych osobowych.

Podmiot przetwarzający | Inaczej: *Procesor*
Podmiot, który przetwarza dane osobowe realizując cel administratora i na jego polecenie.

Odbiorca
Podmiot, któremu ujawnia się dane osobowe. Może być to firma, instytucja, a także osoba fizyczna.

Umowa powierzenia danych
(z ang. skrót: DPA, tj. data processing agreement)
Umowa, na podstawie której administrator danych osobowych powierza procesorowi przetwarzanie danych osobowych.

Profilowanie

Zgodnie z definicją profilowania przyjętą w RODO profilowaniem jest zautomatyzowane przetwarzanie danych osobowych do oceny niektórych czynników osobowych osoby fizycznej. Należy z tego wysnuć dwa wnioski. Pierwszy, profilowanie nie musi się opierać na wyłącznie zautomatyzowanym procesie oraz drugi, profilowanie obejmuje formę oceny danej osoby.

Jak wynika z powołanej definicji oraz z wyjaśnienia zawartego w Wytycznych w sprawie zautomatyzowanego podejmowania decyzji w indywidualnych przypadkach i profilowania do celów rozporządzenia 2016/679/UE z 06.02.2018 – dalej „Wytyczne", na profilowanie składają się trzy elementy:

- zautomatyzowana forma przetwarzania;
- kwalifikacja danych jako dane osobowe w rozumieniu RODO;
- ocena czynników osobowych osoby fizycznej jako cel zautomatyzowanego przetwarzania.

Warto zwrócić uwagę, że w Wytycznych stwierdza się, że: *(...) zwykła klasyfikacja osób fizycznych ze względu na znane cechy, jak np. wiek, płeć i wzrost, nie musi skutkować profilowaniem. Decydujący będzie cel takiej klasyfikacji.*

Zautomatyzowane podejmowanie decyzji

Zautomatyzowane podejmowanie decyzji nie jest tożsame z profilowaniem, może jednak z profilowania wynikać. Zautomatyzowane podejmowanie decyzji może więc, ale nie musi, obejmować profilowanie. Podobnie w drugą stronę, profilowanie może odbywać się bez podjęcia w efekcie zautomatyzowanej decyzji. Przez zautomatyzowane podejmowanie decyzji należy rozumieć proces, w którym nie występuje czynnik ludzki.

W RODO zawarta została gwarancja odnosząca się do takiego działania (art. 22 ust. 1 i ust. 4), a wprowadzona jako prawo Podmiotu danych do tego, by nie podlegać decyzji, która opiera się na wyłącznie zautomatyzowanym przetwarzaniu, w tym profilowaniu (jeżeli wywołuje wobec tej osoby skutki prawne lub w podobny sposób istotnie na nią wpływa). Ta materia została szerzej omówiona w motywie 71 RODO, w którym wskazano jako jeden z przykładów decyzji podejmowanej wyłącznie w oparciu o przetwarzanie zautomatyzowane, tj. elektroniczne metody rekrutacji **bez interwencji ludzkiej**. Należy więc uznać, że w przypadkach, gdy rekrutacja odbywa się przy udziale człowieka, a tym bardziej, gdy to człowiek podejmuje decyzję, zakaz ten nie ma zastosowania.

Należy również zwrócić uwagę, że obowiązki wskazane w art. 13-15 RODO, a związane z profilowaniem ograniczone są do sytuacji, gdy dochodzi do profilowania, o którym mowa w art. 22 ust. 1 i 4 RODO, czyli takiego, które kończy się zautomatyzowanym wydaniem decyzji.

Odmiennie wygląda to w odniesieniu do prawa do sprzeciwu, o którym mowa w art. 21 ust. 1 RODO (pamiętać należy, że prawo to przysługuje w ściśle określonych w RODO przypadkach – zob. strona 22), ponieważ dotyczy każdego profilowania (czyli także tego, które nie prowadzi do zautomatyzowanego wydania decyzji), jednak prawo to zawężone jest do sytuacji, gdy istnieją przyczyny związane ze szczególną sytuacją Podmiotu danych.

Pseudonimizacja
Przetworzenie danych osobowych w taki sposób, by nie można ich było już przypisać konkretnej osobie, której dane dotyczą, bez użycia dodatkowych informacji, pod warunkiem, że takie dodatkowe informacje są przechowywane osobno i są objęte środkami technicznymi i organizacyjnymi uniemożliwiającymi ich przypisanie zidentyfikowanej lub możliwej do zidentyfikowania osobie fizycznej.

Anonimizacja
Anonimizacja stanowi wynik przetwarzania danych osobowych w celu nieodwracalnego uniemożliwienia zidentyfikowania osoby, której dane dotyczą. Zasady ochrony danych nie powinny mieć zastosowania do informacji anonimowych (czyli informacji, które nie wiążą się ze zidentyfikowaną lub możliwą do zidentyfikowania osobą fizyczną), ani do danych osobowych zanonimizowanych w taki sposób, że osób, których dane dotyczą, w ogóle nie można zidentyfikować lub już nie można zidentyfikować. Co do zasady RODO nie dotyczy przetwarzania anonimowych informacji. Niemniej jednak, administrator danych powinien wziąć pod rozwagę planując proces anonimizacji, że zanonimizowane dane mogą nadal stanowić ryzyko naruszenia praw i wolności osoby, której dane dotyczą, np. zastosowanie anonimizacji profili kandydatów do pracy poprzez usunięcie ich tożsamości, podczas gdy historia zawodowa kandydatów pozwala przy użyciu publicznie dostępnych zasobów, czy nawet w wyniku zapytań wprowadzanych do wyszukiwarek, zidentyfikować tożsamość określonych osób. Zaleca się zatem, aby nie traktować anonimizacji jako działania jednorazowego, a jako ciągły proces w którym szczególne znaczenie ma badanie, czy przy aktualnym poziomie myśli technicznej możliwa jest identyfikacja

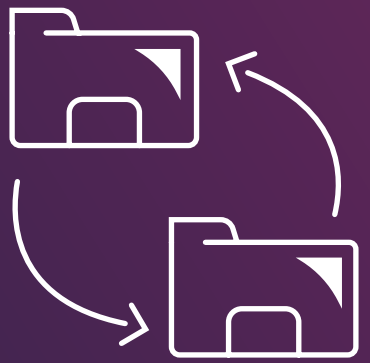
osoby fizycznej, której dane zostały zanonimizowane np. usunięcie efektu zamazanej twarzy na zdjęciu, usunięcie pierwszej warstwy atramentu z zanonimizowanego tekstu itp.

Naruszenie ochrony danych osobowych

Naruszenie ochrony danych osobowych to incydent bezpieczeństwa (informacji) prowadzący do przypadkowego lub niezgodnego z prawem zniszczenia, utracenia, zmodyfikowania, nieuprawnionego ujawnienia lub nieuprawnionego dostępu do przesyłanych, przechowywanych lub w innych sposób przetwarzanych danych osobowych np. wysłanie niezaszyfrowanego maila z danymi osobowymi do nieprawidłowego odbiorcy, zgubienie lub kradzież niezaszyfrowanego laptopa lub pendrive'a, niedostępność danych osobowych spowodowana awarią systemu, zagubienie lub zniszczenie dokumentacji papierowej, ujawnienie haseł dostępu osobom postronnym, pozostawienie dokumentów z danymi osobowymi w drukarce lub skanerze, który zostanie zabrany do serwisu, pozostawienie otwartych pomieszczeń z szafami, gdzie przechowywane są np. dokumenty płacowe, wysłanie maila z widoczną listą mailingową do wielu odbiorców, nieuprawnione przesłanie np. danych osobowych osób trzecich lub treści objętych tajemnicą przedsiębiorstwa przez pracownika na prywatną skrzynkę mailową.

Organ

Organ właściwy w zakresie ochrony danych osobowych. W Polsce organem takim zgodnie z Ustawą z 10.05.2018 r. o ochronie danych osobowych (Dz. U. z 2019 r. poz. 1781) – dalej „Ustawa o ochronie danych osobowych" jest Prezes Urzędu Ochrony Danych Osobowych (www.uodo.gov.pl), będący jednocześnie organem nadzorczym w rozumieniu RODO. Prezes UODO wraz z Europejską Radą Ochrony Danych Osobowych mają wyłączną kompetencję dokonywania oficjalnej interpretacji prawa w zakresie ochrony danych osobowych. Nie mają jej inne organy i instytucje.



Podstawowe zasady przetwarzania danych

3

PODSTAWOWE ZASADY PRZETWARZANIA DANYCH

Ważne:
na agencji zatrudnienia jako na administratorze danych spoczywa obowiązek udowodnienia, że dana osoba wyraziła zgodę, może być to np. mail przesłany przez zainteresowanego w odpowiedzi na ogłoszenie albo zgoda zamieszczona w formularzu aplikacyjnym

Zasada zgodności z prawem – art. 6 RODO

Zgodnie z zasadą zgodności z prawem przetwarzanie danych osobowych może mieć miejsce wyłącznie wtedy, gdy występuje jedna z podstaw prawnych przetwarzania, wskazana w art. 6 RODO. Z punktu widzenia działalności agencji zatrudnienia szczególne znaczenie mają poniższe podstawy prawne:

- **zgoda** na przetwarzanie danych;

  podejmując decyzję o wykorzystaniu zgody jako podstawy przetwarzania, należy pamiętać, iż może ona zostać w dowolnym momencie wycofana przez podmiot danych, a więc z perspektywy administratora obarczona jest ryzykiem związanym z koniecznością usunięcia danych. Dlatego też, przed wykorzystaniem zgody należy rozważyć, czy dla realizacji danego celu nie ma innych podstaw przetwarzania, np. wynikających z obowiązku prawnego.

- podjęcie działań **przed zawarciem umowy** na żądanie podmiotu danych;
- **konieczność wykonania umowy**, której stroną jest osoba, której dane dotyczą (tj. wykonywanie umowy, np. umowy o pracę lub umowy cywilnoprawnej albo umowy z kontrahentem i wszelkich innych rodzajów umów, których wykonanie nie byłoby możliwe bez jednoczesnego przetwarzania danych);
- wypełnienie **obowiązku prawnego ciążącego na administratorze** (np. konieczność przechowywania dokumentów na potrzeby realizacji obowiązków pracodawcy w stosunku do Zakładu Ubezpieczeń Społecznych, Państwowej Inspekcji Pracy i innych instytucji publicznych);
- **prawnie uzasadniony interes** administratora danych (np. zainstalowanie lokalizatorów GPS w samochodach służbowych, wykorzystanie monitoringu wizyjnego na terenie firmy w celu ochrony mienia i personelu, czy aktywnego adresu poczty elektronicznej byłego pracownika).

Wybierając tę przesłankę jako podstawę przetwarzania, należy pamiętać, że przetwarzanie nie

może naruszać podstawowych praw i wolności osoby, której dane dotyczą. Pomocny w ocenie możliwości wykorzystania tej przesłanki może być test równowagi interesów opublikowany przez brytyjskiego regulatora, tj. ICO[1].

Zasada rzetelności, przejrzystości – art. 5 ust. 1 pkt a RODO

W kontekście rzetelności istotne znaczenie mają przede wszystkim odpowiednie środki techniczne i organizacyjne pozwalające na właściwe zabezpieczenie danych osobowych. Ponadto, agencja zatrudnienia powinna dbać o to, aby osoby, których dane są przetwarzane były świadome, kto jest administratorem ich danych oraz jaki jest zakres i cel przetwarzania ich danych. Wszelkie informacje oraz komunikaty powinny być łatwo dostępne oraz sformułowane zrozumiałym językiem, a dodatkowo zwięzłe. Szczególnego znaczenia nabiera obowiązek informacyjny (art. 13, 14 RODO), który nakazuje administratorowi informowanie m. in. o zakresie przetwarzanych danych, celu lub celach przetwarzania (np. rekrutacja, zatrudnienie), odbiorcach lub kategoriach odbiorców danych osobowych (np. pracodawcy użytkownicy, którzy po udostępnieniu danych pracowników tymczasowych administrują tymi danymi). Ponadto, należy poinformować o prawach podmiotów danych wynikających z art. 15-22 RODO, czyli prawie dostępu do danych, prawie do przenoszenia i usuwania danych osobowych, prawie do ograniczenia przetwarzania, jak również prawie do sprzeciwu na ich przetwarzanie, szczególnie w kontekście działań marketingowych.

Zasada ograniczoności celu – art. 5 ust. 1 pkt b RODO

Dane osobowe muszą być zbierane w konkretnych, wyraźnych i prawnie uzasadnionych celach i nie przetwarzane dalej w sposób niezgodny z tymi celami. Agencje zatrudnienia powinny, jeśli jest to konieczne, zbierać osobne zgody od podmiotów danych na konkretne cele, gdy nie ma innej podstawy ich gromadzenia. Dane nie mogą być przetwarzane w niejasnych, trudnych do zdefiniowania celach, których nie można wskazać w sposób dokładny i precyzyjny (w szczególności w celach niezwiązanych ze świadczonymi usługami, ale np. wyłącznie z działalnością kontrahenta).

1 https://ico.org.uk/media/for-organisations/forms/2258435/gdpr-guidance-legitimate-interests-sample-lia-template.docx

Zasada minimalizacji danych – art. 5 ust. 1 pkt c RODO

Dopuszczalny zakres przetwarzanych danych musi być adekwatny i ograniczony wyłącznie do takiego katalogu danych, który jest niezbędny do osiągnięcia celów, dla których dane są przetwarzane. Agencje zatrudnienia powinny mieć na uwadze, że nie należy kopiować i przechowywać kopii dokumentów tożsamości lub innych dokumentów pozwalających na identyfikację osoby[2] (np. dowodów osobistych, praw jazdy, legitymacji) zatrudnianych osób, gdyż nie jest to konieczne, aby ustalić tożsamość zatrudnionej osoby i nie służy innym celom związanym z zatrudnieniem. Wyjątek stanowi proces zatrudnienia cudzoziemców, gdzie przepisy prawa zobowiązują pracodawcę do przechowywania kopii paszportu, czy wizy.

Nie powinno również mieć miejsca zbieranie od osób ubiegających się o zatrudnienie danych innych, niż przewidziane w przepisach prawa chyba, że osoba, której dane dotyczą sama udostępniła swoje dane (np. fotografię w CV), co oznacza, że wyraziła na to swoją dobrowolną zgodę.

Zasada prawidłowości – art. 5 ust. 1 pkt d RODO

Dane osobowe muszą być prawidłowe i w razie potrzeby uaktualniane. Należy podjąć wszelkie rozsądne działania, aby dane osobowe, które są nieprawidłowe w świetle celów ich przetwarzania, zostały niezwłocznie usunięte lub sprostowane. Jest to szczególnie istotne z punktu widzenia przetwarzania danych osobowych na potrzeby instytucji publicznych (np. Zakład Ubezpieczeń Społecznych, właściwy urząd skarbowy), albowiem np. w toku postępowań kontrolnych, organy winny mieć dostęp do aktualnych, nie wprowadzających w błąd danych. Można to osiągnąć np. poprzez cykliczne powiadomienia wysyłane do pracowników z prośbą o uaktualnienie danych lub mailingi do kandydatów.

Zasada ograniczenia przechowywania – art. 5 ust. 1 pkt e RODO

Dane osobowe muszą być przechowywane w formie umożliwiającej identyfikację osoby, której dane dotyczą nie dłużej, niż jest to niezbędne do celów,

2 Nieuprawnione kopiowanie i przechowywanie kopii dokumentu podlega odpowiedzialności karnej na podstawie art. 58 Ustawy z 22.11.2018 r. o dokumentach publicznych (Dz. U. z 2019 r. poz. 53).

Ważne:
Nie jest rekomendowane długie przechowywanie danych, z których w ogóle nie korzystamy. **Rekomendujemy usuwanie danych kandydatów, z którymi agencja nie podjęła kontaktu przez 2 lata od ich zebrania**. Każda agencja, biorąc pod uwagę specyfikę swojej działalności i charakter realizowanych procesów rekrutacyjnych (w tym rodzaj lub poziom stanowisk, stopień trudności w ich pozyskaniu, długość trwania procesu rekrutacyjnego, czy wskaźnik rotacji w danym rodzaju/szczeblu stanowiska) może podjąć samodzielną decyzję o tym, czy okres retencji danych skrócić czy wydłużyć; przy wydłużeniu musi jednak umieć wykazać, jakie kryteria, cele lub inne przesłanki o charakterze obiektywnym to uzasadniają.

dla których dane te są przetwarzane, przy czym:

- dane osobowe można przechowywać przez okres dłuższy, o ile będą one przetwarzane wyłącznie do celów archiwalnych w interesie publicznym, do celów badań naukowych lub historycznych lub do celów statystycznych, pod warunkiem wdrożenia odpowiednich środków technicznych i organizacyjnych, czyli rozdzielenia baz danych ze względu na wymienione cele. Administrator danych powinien ustalić termin ich usuwania (tzw. okres retencji) lub okresowego przeglądu.

W działalności agencji zatrudnienia niektóre dane osobowe musimy przechowywać obowiązkowo i przez czas określony przepisami obowiązującego prawa. Dotyczy to na przykład akt osobowych, dokumentacji podatkowej lub ubezpieczeniowej pracowników. **W przypadku, gdy przepis prawa nie wskazuje obowiązkowego okresu przechowywania, każdy podmiot musi zdecydować samodzielnie o okresie przechowywania danych, uwzględniając przy tym cel w jakim je przetwarza**. W szczególności dotyczy to danych, które zbieramy na potrzeby podstawowych celów naszej działalności, czyli danych kandydatów i klientów. RODO nie wskazuje minimalnego lub maksymalnego okresu przechowywania takich danych. Dlatego każda agencja musi samodzielnie zdecydować, jak długo będzie przechowywała określone kategorie danych.

W przypadku przetwarzania danych osoby kontaktowej reprezentującej naszego klienta, można je przetwarzać na podstawie prawnie uzasadnionego interesu, którym jest dążenie do realizacji umowy. Po okresie realizacji umowy również możliwe jest ich dalsze przetwarzanie, jeżeli ma to nadal związek z umową, np. dochodzenie roszczeń, regulowanie należności, obsługa reklamacji i gwarancji. Natomiast kontakt z taką osobą do celów handlowych lub marketingowych (np. złożenie oferty na nową usługę, pierwszy kontakt z potencjalnym klientem) możliwy jest, jeżeli posiadamy wcześniej udzielone zgody na konkretnie sprecyzowane działania (np. na przesyłanie treści marketingowych mailem) oraz gdy osoba ta udzieli zgody na przetwarzanie jej danych w tym celu, chyba że administrator danych jako podstawę prawną przyjął swój prawnie uzasadniony interes. Wtedy konieczne jest poinformowanie takiej osoby o jej prawie do sprzeciwu.

Zasada integralności i poufności danych – art. 5 ust. 1 pkt f RODO

Dane osobowe muszą być przetwarzane za pomocą odpowiednich środków technicznych i organizacyjnych, w sposób zapewniający tym danym odpowiednie bezpieczeństwo i poufność, w tym ochronę przed:

- niedozwolonym lub niezgodnym z prawem przetwarzaniem, czyli m.in. nieuprawnionym dostępem do nich oraz do sprzętu służącego ich przetwarzaniu, a także przed nieuprawnionym korzystaniem z tych danych i ze sprzętu,
- przypadkową utratą, zniszczeniem lub uszkodzeniem.

Szczególnie ważne jest, aby dane osobowe nie trafiały do osób nieupoważnionych oraz nie przedostały się do obrotu publicznego. Na podmiotach przetwarzających dane (zarówno administratorach, jak i procesorach) ciąży obowiązek stosowania odpowiednich środków i polityk gwarantujących bezpieczeństwo danych osobowych, przy czym przepisy nie przewidują zamkniętego katalogu tego rodzaju środków.

Wybrane środki techniczne i organizacyjne ochrony danych osobowych zostały przedstawione w Suplemencie (Rozdział IX).

Zasada rozliczalności – art. 5 ust. 2 RODO

Każdy administrator danych musi być w stanie wykazać przestrzeganie przepisów RODO. Po stronie administratora leży wykazanie, że przestrzega RODO i innych przepisów o ochronie danych osobowych, np. w przypadku kandydatów do pracy administrator powinien wykazać, że **uzyskał** zgodę na przetwarzanie danych osobowych i **spełnił** względem nich obowiązek informacyjny. W przypadku osób kontaktowych po stronie klientów, administrator również powinien wykazać się spełnieniem obowiązku informacyjnego. Administrator musi być także w stanie udowodnić przestrzeganie, opisanego w art. 25 RODO, obowiązku uwzględniania ochrony danych w fazie projektowania oraz zapewnienia domyślnej ochrony danych.

Prawa osób, których dane dotyczą

4

PRAWA OSÓB, KTÓRYCH DANE DOTYCZĄ

Ważne:
Udostępnienie danych osobowych nieuprawnionemu odbiorcy stanowi naruszenie ochrony danych, dlatego agencja szczególną uwagę powinna poświęcić weryfikacji, czy wniosek dotyczący realizacji jednego z praw przysługujących na mocy RODO pochodzi od uprawnionej osoby i nie stanowi próby wyłudzenia danych osobowych.

Osoba, której dane dotyczą może żądać od agencji zatrudnienia realizacji wszystkich przysługujących jej praw, które zostały wymienione w niniejszym rozdziale. Przed wykonaniem żądania oraz biorąc pod uwagę cel przetwarzania agencja ocenia, czy:

- tożsamość zgłaszającego może zostać potwierdzona na podstawie danych zawartych we wniosku, a jeżeli nie, wówczas agencja dokłada rozsądnych starań, aby te dane potwierdzić; brak możliwości potwierdzenia danych elektronicznie uzasadnia konieczność osobistego wezwania składającego żądanie;
- przechowywanie określonych danych osobowych nie jest wymagane przez przepisy prawa;
- interes agencji nie jest nadrzędny względem interesu składającego żądanie (np. potencjalne roszczenia);
- składający żądanie nie wprowadza agencji w celowy błąd mogący narazić agencję na konsekwencje prawne lub stratę.

Administrator danych osobowych ma prawo zażądać od osoby składającej wniosek o realizację praw, sprecyzowania wniosku, jeżeli dotyczy to sytuacji przetwarzania bardzo dużej ilości danych osobowych i istnieje kilka podstaw prawnych przetwarzania.

Agencja ma obowiązek udzielić osobie, której dane dotyczą, informacji o działaniach podjętych w związku z jej żądaniem niezwłocznie, ale nie później niż w terminie jednego miesiąca od otrzymania żądania. Termin realizacji może zostać wydłużony maksymalnie o kolejne 2 miesiące w sytuacjach skomplikowanego charakteru lub dużego wolumenu żądań. W każdej takiej sytuacji, administrator informuje osobę, której dane dotyczą w ciągu miesiąca od otrzymania żądania o wydłużeniu realizacji i przyczynach opóźnienia lub przyczynach niepodjęcia działań.

Dobrą praktyką przy wnioskach mailowych jest zastosowanie automatycznej informacji zwrotnej potwierdzającej wpłynięcie wniosku.

Zasadniczo realizacja praw podmiotów danych przez administratora odbywa się bezpłatnie. Oznacza to, że administrator nie pobiera opłat za spełnienie

żądania lub udzielenie informacji. Wyjątkowo, administrator może pobrać z tego tytułu rozsądną, niewygórowaną opłatę, jeśli żądania osoby, której dane dotyczą są nieuzasadnione lub nadmierne, w szczególności, jeżeli są ustawiczne albo żądający zwróci się o kolejne kopie swoich danych osobowych. Opłata nie powinna przewyższać zwykłych kosztów administracyjnych, poniesionych na spełnienie żądania (koszty wysyłki, koszty wykonania kopii itd.).

Prawo do informacji – art. 12 – 14 RODO

Administrator danych jest obowiązany udzielać osobie żądającej informacji w zwięzłej, przejrzystej, zrozumiałej i łatwo dostępnej formie, jasnym i prostym językiem. Osoba, której dane dotyczą, ma prawo oczekiwać informacji m. in. o tożsamości administratora, celach i podstawie prawnej przetwarzania, a także o możliwości wycofania zgody udzielonej na przetwarzanie danych.

Prawo dostępu do danych – art. 15 RODO

Osoba, której dane dotyczą jest uprawniona do uzyskania od administratora danych potwierdzenia, czy przetwarza on dane osobowe, które jej dotyczą. Jeżeli tak, osoba ta może żądać np. udzielenia jej informacji o celu przetwarzania, czy też czasie, w jakim dane będą przetwarzane. Administrator ma obowiązek wydać podmiotowi żądającemu kopię jego danych, przy czym domyślną formą wydania kopii jest kopia elektroniczna. Kopia danych powinna być przygotowana w powszechnie stosowanym i możliwym do odczytu pliku, np. plik csv, xls lub pdf.

Prawo do sprostowania danych – art. 16 RODO

Osoba, której dane dotyczą może w dowolnym momencie żądać od agencji zatrudnienia, z uwzględnieniem celów przetwarzania, sprostowania dotyczących jej danych osobowych, które są nieprawidłowe lub ich uzupełnienia, jeżeli są niekompletne.

Powyższe prawo jest realizowane w sposób elektroniczny lub osobiście poprzez wypełnienie dedykowanego formularza (oświadczenia).

Prawo do usunięcia danych (bycia zapomnianym) – art. 17 RODO

Osoba, której dane dotyczą może w dowolnym momencie żądać od agencji usunięcia wszystkich dotyczących jej danych osobowych.

Prawo do bycia zapomnianym realizowane jest poprzez usunięcie wszelkich danych osobowych osoby, której dane dotyczą, włączając w to wszystkie bazy wewnętrzne agencji. Nadto agencja musi dołożyć wszelkich starań, aby podmioty przetwarzające dokonały takiego usunięcia w swoich bazach danych.

Agencja w sposób jasny i publicznie dostępny musi zapewnić możliwość kontaktu w celu realizacji powyższych praw. Może to zrobić w formie formularza papierowego, na stronie internetowej lub dedykowanego adresu e-mail (rekomenduje się podanie co najmniej dwóch alternatywnych form kontaktu). Należy wziąć pod uwagę to, czy osoby których dane przetwarzamy będą miały możliwość łatwego dotarcia do danych administratora, np. czy są to osoby, które mają dostęp do Internetu, czy tablica na której wisi informacja jest ogólnie dostępna dla każdego z adresatów jej treści itp.

Prawa powyższe są realizowane w sposób elektroniczny lub osobiście poprzez bezpośrednie przesłanie żądania z danymi umożliwiającymi identyfikację składającego żądanie. Szczególne ograniczenia w wykonaniu prawa do zapomnienia występują w odniesieniu do pracowników i byłych pracowników. W tym zakresie sposób i czas przetwarzania danych osobowych jest regulowany odrębnymi przepisami, np. w odniesieniu do dokumentacji pracowniczej[3] (co do zasady 10 lub 50 lat); protokołu ustalenia okoliczności i przyczyn wypadku przy pracy wraz z dokumentacją powypadkową (10 lat); nagrania monitoringu (3 miesiące) czy kopii deklaracji rozliczeniowych i imiennych raportów miesięcznych składanych do ZUS (5 lat).

Prawo do sprzeciwu – art. 21 RODO

Prawo to przysługuje wyłącznie osobie, której dane przetwarzane są:

- w interesie publicznym lub w ramach sprawowania władzy publicznej,
- do celów wynikających z prawnie uzasadnionych interesów realizowanych przez administratora lub osobę trzecią,
- do celów marketingu bezpośredniego.

Zgłoszenie sprzeciwu w powyższych sytuacjach powoduje, że dalsze przetwarzanie danych stanie się co do zasady niemożliwe.

3 Na dokumentację pracowniczą składają się akta osobowe oraz dokumentacja w sprawach związanych ze stosunkiem pracy np. ewidencja czasu pracy.

Ważne: prawo do sprzeciwu nie przysługuje osobie, której dane są przetwarzane na podstawie zgody (np. kandydatowi w procesie rekrutacyjnym) lub w związku z realizacją umowy (np. osobie kontaktowej klienta w związku z realizacją umowy). W stosunku to tych osób, aby uniknąć wprowadzenia w błąd, w obowiązku informacyjnym nie powinno się wskazywać prawa do sprzeciwu (osoby te mają jednak prawo do wycofania zgody).

Prawo do sprzeciwu wobec przetwarzania danych do celów marketingu bezpośredniego powinno być zakomunikowane osobie, której dane dotyczą oddzielnie i w sposób zrozumiały.

Prawo do ograniczenia przetwarzania danych – art. 18 RODO

Osoba, której dane dotyczą, ma prawo żądania od administratora ograniczenia przetwarzania jej danych, między innymi:

- jeżeli kwestionuje prawidłowość danych osobowych lub jeżeli przetwarzanie jest niezgodne z prawem, a osoba, której dane dotyczą, sprzeciwia się usunięciu danych osobowych, żądając w zamian ograniczenia ich wykorzystywania.

  Przykład:
  Jeśli pracownik zgłasza błąd w swoim nazwisku, to do czasu poprawienia nazwiska we wszystkich systemach, błędne dane mogą być przeniesione do innego systemu lub oznaczone „do poprawy" tak, aby osoby mające dostęp do systemów informatycznych nie korzystały z błędnych danych.
- gdy administrator nie potrzebuje już danych osobowych do celów przetwarzania, ale są one potrzebne osobie, której dane dotyczą do ustalenia, dochodzenia lub obrony roszczeń.

  Przykład:
  Jeśli pracownik pozostawił w kwestionariuszu osobowym dane osoby do kontaktu alarmowego (np. imię, nazwisko, nr telefonu), po zakończeniu zatrudnienia były pracownik może zwrócić się z wnioskiem o ograniczenie przetwarzania tych danych.

Prawo do przenoszenia danych – art. 20 RODO

Osoba, której dane dotyczą, ma prawo żądania otrzymania w ustrukturyzowanym, powszechnie używanym formacie (np. csv, xls), nadającym się do odczytu maszynowego, danych osobowych jej dotyczących oraz przesłania ich innemu administratorowi bez przeszkód ze strony administratora, któremu dostarczono te dane osobowe. Poza tym, ma prawo żądać przesłania danych bezpośrednio między administratorami, o ile jest to technicznie możliwe.

Aby podmiot danych mógł skorzystać z tego uprawnienia muszą być spełnione łącznie następujące warunki:

- przetwarzanie odbywa się na podstawie zgody lub na podstawie umowy,
- przetwarzanie odbywa się w sposób zautomatyzowany.

Wykonywanie prawa do przenoszenia danych nie może niekorzystnie wpływać na prawa i wolności innych.

Prawo do bycia poinformowanym o tym, że administrator sprostował, usunął lub ograniczył przetwarzanie danych – art. 19 RODO

Administrator ma obowiązek poinformowania o sprostowaniu, usunięciu lub ograniczeniu przetwarzania każdego odbiorcę, któremu ujawniono dane osobowe (chyba, że okaże się to niemożliwe lub będzie wymagać niewspółmiernie dużego wysiłku), a jeżeli zainteresowany tego zażąda, należy poinformować go o odbiorcach, którym ujawniono dane.

Prawo do niebycia poddanym zautomatyzowanej decyzji – art. 22 RODO

Każda osoba, której dane dotyczą, ma prawo do tego, **aby nie podlegać decyzji, która opiera się wyłącznie na zautomatyzowanym przetwarzaniu jej danych, w tym profilowaniu.** Zakaz podejmowania automatycznych decyzji, o którym mowa w art. 22 RODO, wymaga spełnienia dwóch przesłanek łącznie:

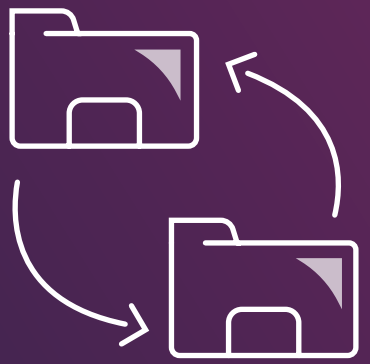
- decyzja, której podmiot danych miałby podlegać, opiera się wyłącznie na zautomatyzowanym przetwarzaniu, w tym profilowaniu (tj. bez merytorycznego udziału człowieka), oraz
- decyzja ta wywołuje wobec podmiotu danych skutki prawne lub w podobny sposób na nią wpływa.

Aby móc poddać podmiot danych decyzji, która opiera się na wyłącznie zautomatyzowanym przetwarzaniu (w tym profilowaniu), należy spełnić jedną z przesłanek z art. 22 ust. 2 RODO, np. pozyskać wyraźną zgodę podmiotu danych.

Konsekwencje niespełnienia żądań podmiotów danych

W przypadku, gdyby administrator nie spełnił żądania uzupełnienia, uaktualnienia, sprostowania danych albo czasowego lub stałego wstrzymania ich przetwarzania, osoba, której dane dotyczą, ma prawo złożyć do organu nadzorczego wniosek o nakazanie dopełnienia tego obowiązku.

W agencjach zatrudnienia, które korzystają z baz danych i systemów wspierających rekrutację na zasadzie „wyszukiwarki" (poprzez wprowadzenie odpowiednich kryteriów wyszukiwania tzw. tagów uzyskuje się zbiór kandydatów spełniających wpisane kryteria), nie mamy do czynienia z tzw. profilowaniem kwalifikowanym (o którym mowa w art. 22 RODO), wymagającym uzyskania wyraźnej zgody kandydata, ponieważ korzystanie z systemów baz danych kandydatów jest co do zasady elementem współistniejącym z czynnikiem ludzkim, a decyzja, który kandydat zostanie zarekomendowany klientowi lub który pracownik zostanie zatrudniony w celu skierowania go do klienta, jest podejmowana przez człowieka. W większości prowadzonych procesów rekrutacji pracownik agencji aktywnie bierze w nim udział poprzez to, że analizuje profile kandydatów i z grupy kandydatów spełniających kryteria samodzielnie wybiera, na podstawie własnej wiedzy i doświadczenia, tych, których rekomenduje klientowi.



Przetwarzanie danych w agencjach zatrudnienia

5

PRZETWARZANIE DANYCH W AGENCJACH ZATRUDNIENIA

USŁUGI REKRUTACYJNE

Charakterystyka usługi

Rekrutacja – usługa doradztwa personalnego i/lub pośrednictwa pracy to usługa zdefiniowana w art. 18 ust. 1 Ustawy o promocji zatrudnienia, polegająca m.in. na inicjowaniu i organizowaniu kontaktów osób poszukujących odpowiedniego zatrudnienia lub innej pracy zarobkowej z pracodawcami, udzielaniu pomocy osobom w uzyskaniu odpowiedniego zatrudnienia oraz pracodawcom w pozyskaniu pracowników o poszukiwanych kwalifikacjach zawodowych, jak również na udzielaniu pracodawcom informacji o kandydatach do pracy, w związku ze zgłoszoną ofertą pracy (pośrednictwo pracy) i na określaniu kwalifikacji pracowników i ich predyspozycji oraz weryfikacji kandydatów pod względem oczekiwanych kwalifikacji (doradztwo personalne).

Podstawowe role pełnione przez agencję i klientów usług rekrutacyjnych

W procesie świadczenia usług rekrutacyjnych agencja pełni rolę administratora danych w stosunku do danych osobowych kandydatów do pracy. Rola administratora danych wynika z istoty działalności prowadzonej przez agencję na podstawie Ustawy o promocji zatrudnienia, tj. świadczenia **usług pośrednictwa pracy** polegających m.in. na organizowaniu kontaktów osób poszukujących odpowiedniego zatrudnienia z pracodawcami, a także na udzielaniu pracodawcom informacji o kandydatach do pracy, oraz **usług doradztwa personalnego** polegających m. in. na określaniu kwalifikacji pracowników i ich predyspozycji, jak również weryfikacji kandydatów pod względem oczekiwanych kwalifikacji.

Powyższe usługi agencja wykonuje na potrzeby **wszystkich rekrutacji prowadzonych na rzecz swoich obecnych i przyszłych klientów**. Realizuje ona zatem **własne**

cele przetwarzania, posługując się przy tym **własnymi środkami** i metodami, w tym środkami technologicznymi (bazy danych kandydatów, poszukiwania bezpośrednie i pośrednie, testy, formularze, analizy).

W celu świadczenia usług rekrutacyjnych, w szczególności zarekomendowania klientom kandydatów spełniających oczekiwane wymagania, **agencja udostępnia dane osobowe tych kandydatów klientowi, działającemu jako samodzielny administrator danych**. Klient agencji, po otrzymaniu od niej danych osobowych proponowanych kandydatów, zaczyna **realizować własny cel przetwarzania**, jakim jest weryfikacja i ocena danych, a także samodzielne podjęcie decyzji o zatrudnieniu lub odrzuceniu danej kandydatury. **Jest zatem również w pełni odrębnym administratorem danych, decydującym o celach** (zatrudnienie pracownika o poszukiwanych cechach) i **środkach przetwarzania** (własna baza danych, analiza dokumentów, spotkanie z kandydatem, wideokonferencja itd.).

Mając na uwadze powyższe, w procesie rekrutacji pomiędzy agencją a klientem zachodzi relacja administrator – administrator, a wymiana danych powinna następować na zasadzie udostępnienia. Każdy podmiot realizuje bowiem własny cel i posługuje się własnymi środkami przetwarzania danych.

Warunki konieczne przetwarzania danych kandydatów w procesie rekrutacji:

- zgoda kandydata (art. 6 pkt 1 lit. a RODO),
- dopełnienie obowiązku informacyjnego przez agencję (art. 13 RODO),
- dopełnienie obowiązku informacyjnego przez klienta (art. 14 RODO).

Kandydat może udzielić zgody na wszystkie procesy rekrutacyjne prowadzone przez agencję, co daje możliwość udostępniania jego danych wielu potencjalnym pracodawcom. W takiej sytuacji dane kandydata najczęściej umieszczane są w bazie kandydatów agencji, a ich przetwarzanie oparte jest na ogólnej zgodzie kandydata na korzystanie z jego danych do procesów rekrutacyjnych. Dobrą praktyką biznesową jest potwierdzanie akceptacji kandydata na udostępnienie jego danych konkretnym klientom, których agencja chce zarekomendować do pracy.

Prawem kandydata jest także wyrażenie zgody wyłącznie na jeden proces rekrutacyjny, w którym chce wziąć udział. Aplikując na ogłoszenie do konkretnej pracy lub firmy, kandydat może zgodzić się, aby jego dane osobowe były przetwarzane wyłącznie w tym procesie, przesłanie CV jest wówczas jednoznaczne z wyrażeniem zgody na przetwarzanie danych wyłącznie

w ramach konkretnego procesu rekrutacyjnego. W takiej sytuacji agencja nie może przetwarzać danych tego kandydata w innych procesach rekrutacyjnych oraz przetwarzać jego danych w bazie po zakończeniu określonej rekrutacji.

PRACA TYMCZASOWA

Charakterystyka usługi

Praca tymczasowa usługa zdefiniowana w Ustawie z 9.07.2003 r. o zatrudnianiu pracowników tymczasowych (Dz. U. z 2018 r., poz. 594) – dalej „UZPT", polegająca na zatrudnianiu pracowników tymczasowych (zatrudnionych w oparciu o umowę o pracę lub umowę cywilnoprawną) i kierowaniu ich do wykonywania pracy tymczasowej na rzecz i pod kierownictwem pracodawcy użytkownika.

Podstawowe role pełnione przez agencję i pracodawcę użytkownika

Na etapie rekrutacji do pracy tymczasowej agencja pracy tymczasowej pełni rolę administratora danych osobowych kandydatów.

Po zatrudnieniu pracownika tymczasowego w celu skierowania go do wykonywania pracy tymczasowej na rzecz pracodawcy użytkownika, agencja pracy tymczasowej jest administratorem jego danych osobowych jako pracodawca przez cały okres zatrudnienia, a następnie po jego ustaniu jako były pracodawca.

Rolę pracodawcy użytkownika w procesie przetwarzania danych pracowników tymczasowych należy analizować z uwzględnieniem przepisów Ustawy o zatrudnianiu pracowników tymczasowych. W ustawie tej występuje nietypowa dla tradycyjnego stosunku pracy relacja trzech podmiotów: pracownika tymczasowego, pracodawcy, którym jest agencja pracy tymczasowej i pracodawcy użytkownika. Specyfikę tej relacji tworzy w szczególności zawarcie umowy o pracę przez jeden podmiot (agencję pracy tymczasowej) wyłącznie w celu skierowania do wykonywania pracy na rzecz innego podmiotu (pracodawcy użytkownika) oraz nadzór i kierownictwo sprawowane przez pracodawcę użytkownika, a nie przez podmiot zatrudniający. To „rozszczepienie" obowiązków pracodawcy ma szczególne znaczenie w kontekście definicji stosunku pracy, określonej w art. 22 Ustawy z 26.06.1974 r. – Kodeksu pracy – dalej „KP". Zgodnie

z tym przepisem „*Przez nawiązanie stosunku pracy pracownik zobowiązuje się do wykonywania pracy określonego rodzaju na rzecz pracodawcy i pod jego kierownictwem oraz w miejscu i czasie wyznaczonym przez pracodawcę, a pracodawca do zatrudniania pracownika za wynagrodzeniem*". Powyższa definicja doznaje istotnej modyfikacji na gruncie UZPT, gdyż zasadnicze elementy stosunku pracy, wymienione w przywołanym art. 22 KP, jak wykonywanie pracy określonego rodzaju, wykonywanie pracy „na rzecz", kierownictwo nad pracownikami oraz wyznaczanie miejsca i czasu wykonywania pracy leżą po stronie pracodawcy użytkownika, co licznie potwierdzają przepisy ustawy o UZPT, a w szczególności art. 2 pkt 2, który potwierdza to wprost. Powyższe nakazuje uznać, że rola pracodawcy, wynikająca z definicji z art. 22 KP, jest realizowana w zasadniczej części przez pracodawcę użytkownika, którą wykonuje we własnym imieniu, za pomocą własnych środków i dla osiągnięcia własnych celów gospodarczych. Żaden bowiem przepis prawa pracy nie stanowi, że rolę pracodawcy opisaną w art. 22 KP pracodawca użytkownik wypełnia w imieniu agencji, na zasadzie zlecenia. Nie ma zatem żadnych podstaw – w szczególności w świetle powyższej definicji, aby uznać go za podmiot, który prawa i obowiązki pracodawcy, wynikające z ww. przepisu realizuje jako podmiot przetwarzający.

Wśród istotnych ustawowych praw i obowiązków pracodawcy użytkownika, które w sposób nie budzący wątpliwości przemawiają za uznaniem pracodawcy użytkownika za pełnoprawnego, pełnowymiarowego administratora danych osobowych pracowników tymczasowych należy wymienić między innymi następujące:

- pracodawca użytkownik sprawuje nadzór i kierownictwo nad pracownikiem tymczasowym na takich samych zasadach, jak wykonuje je tradycyjny pracodawca, co oznacza, że ma prawo wydawać pracownikowi tymczasowemu bieżące polecenia służbowe, zarządzać jego czasem pracy itd. (art. 2 pkt 1);
- pracodawca użytkownik wyznacza pracownikowi tymczasowemu zadania i kontroluje ich wykonanie (art. 2 pkt. 1 UZPT);
- pracodawca użytkownik informuje agencję zatrudnienia o wynagrodzeniu, jakie ma być wypłacane pracownikowi tymczasowemu (art. 9 ust. 2 pkt 1 UZPT);
- pracodawca użytkownik wykonuje obowiązki i korzysta z praw przysługujących pracodawcy w zakresie niezbędnym do organizowania pracy z udziałem pracownika tymczasowego (art. 14 ust. 1 UZPT);
- pracodawca użytkownik jest obowiązany

zapewnić pracownikowi tymczasowemu bezpieczne i higieniczne warunki pracy w miejscu wyznaczonym do wykonywania pracy tymczasowej (art. 14 ust. 2 pkt 1 UZPT);

- pracodawca użytkownik prowadzi ewidencję czasu pracy pracownika tymczasowego w zakresie i na zasadach obowiązujących w stosunku do pracowników (art. 14 ust. 2 pkt 2 UZPT);
- pracodawca użytkownik prowadzi ewidencję osób wykonujących pracę tymczasową (art. 14 a UZPT);
- poprzez sprawowanie nadzoru nad przebiegiem pracy, pracodawca użytkownik może współdecydować np. o przyznaniu premii lub nagrody (art. 2 pkt. 1 i art. 14 ust. 1 UZPT);
- pracodawca użytkownik dostarcza pracownikowi tymczasowemu odzież i obuwie robocze oraz środki ochrony indywidualnej, zapewnia napoje i posiłki profilaktyczne, przeprowadza szkolenia BHP, ustala okoliczności i przyczyny wypadku przy pracy, przeprowadza ocenę ryzyka zawodowego oraz informuje o tym ryzyku (art. 9 ust. 2a UZPT);
- pracodawca użytkownik ma obowiązek stosować wobec pracowników tymczasowych tzw. zasadę równego traktowania (art. 15 UZPT).

Nie ma również żadnych przeszkód, aby zakres praw i obowiązków pracodawcy użytkownika został poszerzony w umowie o świadczenie usług zawartej z agencją. Ponadto, należy także przywołać przepis art. 5 UZPT, zgodnie z którym w zakresie nieuregulowanym odmiennie przepisami UZPT do pracodawcy użytkownika (a nie tylko do agencji pracy tymczasowej) stosuje się odpowiednio przepisy prawa pracy dotyczące pracodawcy.

Powyższe wyliczenie praw i obowiązków pracodawcy użytkownika jednoznacznie wskazuje, że praktycznie od momentu przekazania pracodawcy użytkownikowi listy pracowników tymczasowych, którzy stawią się do pracy w jego zakładzie, pracodawca użytkownik zaczyna przetwarzać dane tych pracowników wyłącznie dla własnych celów związanych z prowadzeniem własnego przedsiębiorstwa, we własnym imieniu, przy pomocy własnych środków i wykonując w stosunku do tych osób obowiązki pracodawcy. Pracodawca użytkownik jest także jedynym odbiorcą pracy pracownika tymczasowego i tylko on korzysta z jej materialnych efektów. Jest to samodzielna rola, w której pracodawca użytkownik nie działa na zlecenie agencji, ani nie wykonuje czynności w jej imieniu. W praktyce można by mnożyć przykłady działania pracodawcy użytkownika na własny rachunek z wykorzystaniem danych osobowych pracowników tymczasowych, np. wydawanie bieżących poleceń

służbowych, przypisywanie podległości pracownika tymczasowego w strukturze pracodawcy użytkownika, prowadzenie szkoleń wprowadzających oraz szkoleń z zakresu BHP, ustalanie rozkładów i harmonogramów czasu pracy oraz prowadzenie ewidencji czasu pracy, prowadzenie postępowania w sprawie ustalenia okoliczności i przyczyn wypadku przy pracy oraz sporządzanie protokołów powypadkowych, prowadzenie ewidencji okresów zatrudnienia, wydawanie kart dostępowych do zakładu pracy, wydawanie identyfikatorów pracownika, sporządzanie list pracowników na poszczególnych zmianach, stosowanie do pracowników regulaminów premiowania obowiązujących u pracodawcy użytkownika, uwzględnianie pracowników tymczasowych w planach benefitowych pracodawcy użytkownika, przekazywanie list zatrudnionych pracowników związkom zawodowym, raportowanie danych o takich pracownikach do własnych struktur organizacyjnych itd.

Mając na uwadze powyższe i w zakresie wykonania wszystkich powołanych wyżej czynności pracodawca użytkownik **pełni samodzielną rolę administratora danych, działając we własnym celu i posługując się własnymi środkami przetwarzania. Stanowisko takie prezentuje WEC-Europe[4] oraz prawnicy i przedstawiciele praktyki stosowania prawa[5]**.

Oczywiście, pomimo, iż zasadniczo wymiana danych osobowych pomiędzy agencją pracy tymczasowej a pracodawcą użytkownikiem będzie odbywała się na zasadzie udostępnienia danych, mogą wystąpić – po obu stronach – sytuacje, w których jeden z tych podmiotów zleci drugiemu w drodze umowy wykonanie jakiejś czynności prawnej lub faktycznej (np. pracodawca użytkownik przejmie od agencji obowiązek wystawienia skierowania na badania lekarskie, obowiązek wypłacania należności na pokrycie kosztów podróży służbowej, czy zawierania w imieniu agencji umów o podnoszenie kwalifikacji zawodowych z pracownikami tymczasowymi). W tego rodzaju sytuacjach pracodawca użytkownik realizowałby obowiązki, które zgodnie z UZPT spoczywają na agencji i działałaby w zakresie ich realizacji w imieniu i na rzecz

4 World Employment Confederation, Wytyczne World Employment Confederation dotyczące „niezależnego administratora" lub „podmiotu przetwarzającego" jako dostawcy usług HR, https://www.polskieforumhr.pl/wp-content/uploads/2020/11/WEC-Guidelines-on-Independent-Controller-or-Processor-as-HR-provider__PL.pdf (dostęp: 9/11/2020)

5 Marta Murek prawnik w kancelarii Raczkowski Paruch, DANE OSOBOWE Dostęp do danych bez umowy powierzenia z agencją, https://raczkowski.eu/publikacje/2019/Dost%C4%99p%20do%20danych%20bez%20umowy%20powierzenia%20z%20agencj%C4%85.pdf (dostęp 9/11/2020)
Anna Kuś-Kluka, Radca prawny w kancelarii Juvo, Obowiązki Agencji Pracy Tymczasowej i Pracodawcy Użytkownika związane z ochroną danych osobowych, https://hrnews.pl/obowiazki-agencji-pracy-tymczasowej-i-pracodawcy-uzytkownika-zwiazane-z-ochrona-danych-osobowych/ (dostęp 9/11/2020)

agencji. Doszłoby wtedy do przetwarzania danych w charakterze procesora przez pracodawcę użytkownika, co wymagałoby zawarcia odrębnej umowy powierzenia. Takie sytuacje w praktyce nie są jednak często spotykane, gdyż głównym oczekiwaniem pracodawcy użytkownika jest wykonywanie obowiązków formalnych związanych z zatrudnieniem przez agencję, nie zaś samodzielna ich realizacja.

Warunki konieczne do przetwarzania danych pracowników tymczasowych:

- zgoda pracownika na przetwarzanie danych wykraczających poza KP (art. 22^1a-^{1}b KP),
- dopełnienie obowiązku informacyjnego przez agencję (art. 13 RODO),
- dopełnienie obowiązku informacyjnego przez pracodawcę użytkownika (art. 14 RODO).

KIEROWANIE OBYWATELI POLSKICH DO PRACY ZA GRANICĄ U PRACODAWCY ZAGRANICZNEGO

Charakterystyka usługi

Jest to działalność agencji zatrudnienia uregulowana w art. 85 ust. 2 Ustawy o promocji zatrudnienia, polegająca na zawieraniu umów o skierowanie do pracy za granicą obywateli polskich bezpośrednio z pracodawcami zagranicznymi i kierowaniu kandydatów do pracy do tych pracodawców zagranicznych na podstawie pisemnych umów zawieranych przez agencje z osobami kierowanymi.

Podstawowe role pełnione przez agencję zatrudnienia kierującą kandydatów do pracy do pracodawcy zagranicznego i tego pracodawcę.

W ramach kierowania polskich obywateli do pracy za granicą do zagranicznego pracodawcy agencja zatrudnienia zawiera dwa typy umów:

- umowę handlową z klientem agencji, który będzie bezpośrednim pracodawcą zagranicznym dla skierowanego kandydata;
- umowę kierującą do pracy za granicą z kandydatem do pracy.

Pierwszą z umów jest umowa handlowa, w której agencja zobowiązana jest ustalić na piśmie z przyszłym pracodawcą konkretne warunki zatrudnienia wymagane przez polskie prawo np. czas trwania umowy, wymiar czasu pracy, miejsce pracy, rodzaj pracy oraz wynagrodzenie za pracę. Następnie te warunki, uzgodnione z pracodawcą zagranicznym, są przenoszone do

tzw. umowy kierującej o pracę, która zawierana jest z konkretnym kandydatem wybranym do zatrudnienia przez tego pracodawcę. W obu tych procesach następuje wymiana danych osobowych pomiędzy agencją i kandydatem – celem tej wymiany jest rekrutacja kandydata spełniającego wymagania klienta będącego przyszłym pracodawcą, zapoznanie go z warunkami proponowanym przez tego klienta, a w razie jego akceptacji – zawarcie umowy kierującej, w której kandydat otrzymuje gwarancję pracy na określonych warunkach. Rola agencji w tym procesie nie różni się wiele od roli agencji rekrutującej kandydata na pracownika do polskiego pracodawcy, z tym wyjątkiem, że w przypadku kierowania do pracodawcy zagranicznego występuje obowiązek zawarcia tzw. umowy kierującej.

Zarówno w procesie rekrutacji, jak i w procesie zawarcia umowy kierującej agencja zatrudnienia pełni rolę samodzielnego administratora danych kandydata. Pracodawca zagraniczny pełni również rolę samodzielnego administratora danych osobowych, zarówno w procesie poprzedzającym zatrudnienie pracownika, jak i po jego zatrudnieniu. Samodzielnie decyduje on o celach (zatrudnienie pracownika o poszukiwanych cechach) i środkach przetwarzania (własna baza danych, analiza dokumentów, spotkanie z kandydatem, wideokonferencja itd.).

DELEGOWANIE PRACOWNIKÓW DO PRACY ZA GRANICĄ W RAMACH ŚWIADCZENIA USŁUG

Charakterystyka usługi

Delegowanie pracowników do pracy za granicą w ramach swobody świadczenia usług zostało zdefiniowane w Dyrektywie 96/71/WE Parlamentu Europejskiego i Rady z 16.12.1996 r. dotyczącej delegowania pracowników w ramach świadczenia usług – dalej „Dyrektywa 96/71/WE", implementowanej na gruncie polskim Ustawą o delegowaniu pracowników w ramach świadczenia usług z dnia 10.06.2016 r. (Dz. U. z 2016 r. poz. 868). Polega ono na wysyłaniu przez przedsiębiorcę z jednego państwa członkowskiego własnych pracowników w celu tymczasowego świadczenia usługi w przedsiębiorstwie, mającym siedzibę w innym państwie członkowskim (tzw. państwo przyjmujące). Pracownicy delegowani pozostają zatrudnieni w kraju wysyłającym i de facto nie są włączani do rynku pracy państwa przyjmującego. Nie są więc pracownikami migrującymi. Z tego powodu delegowanie odbywa się w ramach swobody świadczenia usług, a nie swobody przepływu osób. Dyrektywa 96/71/WE wyznacza minimalne standardy

zatrudnienia pracowników w sytuacji świadczenia usługi transgranicznej.

Przepisy przewidują kilka form delegowania pracowników w obrębie UE. Poza wysyłaniem pracowników bezpośrednio przez pracodawcę i pod jego kierownictwem, delegowanie może przybrać formę, w ramach której agencja zatrudnienia mająca siedzibę w danym państwie członkowskim wynajmuje pracownika tymczasowego przedsiębiorstwu prowadzącemu działalność gospodarczą lub działającemu na terytorium innego państwa członkowskiego.

Podstawowe role pełnione przez pracodawcę delegującego personel i jego zagranicznego klienta z innego państwa członkowskiego

Delegowanie pracowników w ramach swobody świadczenia usług na podstawie Dyrektywy 96/71/WE co do zasady najczęściej przybiera postać:

- delegowania pracowników bezpośrednio przez ich pracodawcę, w przypadku którego dedykowani pracownicy czasowo świadczą pracę na rzecz zagranicznego kontrahenta pracodawcy (np. w ramach obsługi danego projektu), lub np. na rzecz zagranicznego oddziału pracodawcy, czy np. tzw. zagranicznej spółki matki,
- wysyłania pracowników tymczasowych świadczących pracę na rzecz i pod kierownictwem zagranicznego pracodawcy użytkownika,
- delegowania osób zatrudnionych, które świadczą określone usługi na rzecz ich odbiorców będących osobami fizycznymi, którzy nie mają jednak statusu pracodawcy lub pracodawcy użytkownika.

W powyższych przypadkach, zarówno na etapie rekrutacji, jak i na etapie zatrudnienia, pracodawca (w przypadku zatrudnienia tymczasowego działający w roli agencji zatrudnienia) **występuje w charakterze administratora danych osobowych**. Celem administrowania jest w tym wypadku zatrudnienie danego pracownika i skierowanie go do świadczenia pracy/świadczenia usług w innym państwie członkowskim na rzecz podmiotu trzeciego.

We wspomnianych wariantach odbiorca usługi (np. pracodawca użytkownik, kontrahent pracodawcy, do którego pracownik jest czasowo kierowany), również występuje w charakterze administratora danych osobowych delegowanych pracowników.

W przypadku pracy tymczasowej wynika to z faktu, że po stronie pracodawcy użytkownika występuje

szereg samodzielnych obowiązków i uprawnień, w tym przede wszystkim kierownictwo, wydawanie poleceń, organizowanie i nadzorowanie procesu pracy.

Z kolei w ramach wariantu czasowego kierowania pracownika do świadczenia pracy u zagranicznego kontrahenta, czy też u osoby fizycznej będącej odbiorcą usługi, podmiot ten administruje danymi osób delegowanych, np. na potrzeby weryfikacji jakości pracy, czasu w jakim jest ona świadczona, wydajności procesu pracy.

We wspomnianych przypadkach przekazanie danych osobowych następuje w oparciu o ich **udostępnienie**. Należy w tym wypadku wykluczyć instytucję powierzenia przetwarzania danych osobowych, albowiem każdy z podmiotów działa we własnym imieniu i realizuje własny, odrębny cel.

Rekomendowane jest uzyskanie zgody delegowanego pracownika na udostępnienie jego danych osobowych, odpowiednio zagranicznemu pracodawcy użytkownikowi, kontrahentowi pracodawcy delegującego, odbiorcy usługi.

Przetwarzanie danych osobowych na poszczególnych etapach delegowania pracowników w ramach swobody świadczenia usług

Co do zasady reguły przetwarzania danych osobowych w przypadku delegowania pracowników są zbieżne z tymi, które obowiązują w przypadku przetwarzania danych osobowych obowiązujących w państwie siedziby delegującego pracodawcy.

Na etapie rekrutacji dane osobowe przetwarzane są na podstawie zgody podmiotu danych oraz właściwych przepisów: Kodeksu pracy (w przypadku zatrudnienia w ramach stosunku pracy), Kodeksu cywilnego (w przypadku zatrudnienia na podstawie umowy cywilnoprawnej). Przetwarzanie następuje z inicjatywy kandydata (osobiste dostarczenie lub przesłanie CV, wypełnienie aplikacji online, itp.) lub z inicjatywy podmiotu zatrudniającego (ogłoszenia rekrutacyjne, spotkania rekrutacyjne, itp.).

Na etapie zatrudnienia podstawą przetwarzania danych osobowych jest dany stosunek prawny (stosunek pracy, umowa cywilnoprawna), usprawiedliwiony interes administratora danych, jak również zgoda zatrudnionego.

Wybrane aspekty dodatkowe związane z delegowaniem pracowników w kontekście przetwarzania ich danych osobowych

Na potrzeby delegowania pracownika i potwierdzenia podlegania pod rodzimy system zabezpieczeń społecznych, z udziałem pracodawcy prowadzone jest postępowanie o wydanie dokumentu A1; należy pamiętać, że w toku właściwego postępowania Zakład Ubezpieczeń Społecznych może żądać szeregu informacji na temat pracownika, które wykraczają poza standardowy katalog; podobnie rzecz ma się w przypadku kwestii związanych z rezydencją podatkową delegowanej osoby (np. dane dot. sytuacji rodzinnej niezbędne celem ustalenia ośrodka interesów życiowych).

Zagraniczne systemy dotyczące delegowania, zgłaszania i ewidencjonowania pracowników delegowanych (np. francuski SIPSI, belgijska LIMOSA) z reguły wymagają danych osobowych wykraczających poza standardowy katalog (np. obowiązkowe zdjęcie pracownika delegowanego).

Wielokrotnie zdarza się, że systemy prawne państw przyjmujących wymagają przedstawienia szeregu dokumentów dotyczących delegowanych pracowników (np. kopie dokumentów tożsamości, kopie wiz).

OUTSOURCING

Charakterystyka usługi

Instytucja outsourcingu nie jest uregulowana w polskim prawie. Zgodnie z jednym z poglądów wyrażonych w literaturze, **outsourcing** to metoda organizacji i zarządzania, polegająca na względnie trwałym, długoterminowym, opartym na kontrakcie, **przeniesieniu odpowiedzialności za realizację określonych obszarów działalności gospodarczej (zadań, funkcji lub procesów) na stronę wyspecjalizowanego partnera zewnętrznego**, przy uwzględnieniu dynamicznego, interakcyjnego i partnerskiego charakteru współpracy nakierowanej na uzyskanie korzyści ekonomicznych i jakościowych oraz przy jednoczesnej możliwości rozwijania kluczowych kompetencji przedsiębiorstwa macierzystego, co umożliwia wzmocnienie jego kluczowej działalności, budowanie przewagi konkurencyjnej i rozwój firmy[6].

Agencje zatrudnienia (podobnie jak inne podmioty prowadzące działalność gospodarczą i nieposiadające statusu agencji zatrudnienia), mogą świadczyć na rzecz swoich kontrahentów usługi outsourcingu w rozumieniu nadanym powyżej, które mogą być

realizowane na zasadzie swobody zawierania i wykonywania umów i są obecnie powszechną formą uzupełniania biznesowych potrzeb przedsiębiorców za pomocą dostawców zewnętrznych.

Role podmiotów przetwarzających dane osobowe w usłudze outsourcingu

Usługi świadczone w ramach outsourcingu realizowane są przy wykorzystaniu personelu zaangażowanego na potrzeby realizacji danej usługi (pracowników, zleceniobiorców). Z punktu widzenia przetwarzania danych osobowych, podmiot świadczący usługę jest administratorem danych osobowych personelu zaangażowanego do jej wykonania (zarówno na etapie jego rekrutacji, jak i zatrudnienia).

Odbiorcę danej usługi należy również kwalifikować jako administratora danych osobowych. Wynika to z faktu, że po jego stronie występują własne środki przetwarzania i własne cele, które mogą obejmować m. in.: czynności związane z udostępnieniem lokalu i pomieszczeń, w których są wykonywane usługi, weryfikację jakości, wydajności, czasu trwania usługi oraz środków zaangażowanych przez inwestora do jej wykonania, zaopatrzenie w środki ochrony indywidualnej, ewentualne przekazania narzędzi niezbędnych do realizacji usługi i inne uzasadnione czynności. Wymiana danych osobowych następuje w oparciu o ich **udostępnienie**. Należy w tym wypadku wykluczyć instytucję powierzenia przetwarzania danych, albowiem każdy ze wskazanych powyżej podmiotów działa we własnym imieniu i realizuje odrębny cel. Każdy zatem zobowiązany jest spełnić względem osoby świadczącej usługi obowiązek informacyjny.

LEGALIZACJA ZATRUDNIENIA OBYWATELI PAŃSTW TRZECICH ORAZ ICH DELEGOWANIA DO ŚWIADCZENIA PRACY W INNYCH PAŃSTWACH CZŁONKOWSKICH UE

Charakterystyka

Jednym z elementów usług świadczonych przez agencje zatrudnienia jest wykonywanie czynności z zakresu legalizacji pobytu i zatrudnienia obywateli państw trzecich (np. obywateli Ukrainy).

Po dokonaniu wspomnianej legalizacji obywatele ci

6 Matejun M., Outsourcing, [w:] Szymańska K. (red.), Kompendium metod i technik zarządzania. Teoria i ćwiczenia, Oficyna Wolters Kluwer business, Warszawa 2015.

mogą między innymi:

- zostać **zatrudnieni przez agencję zatrudnienia jako pracownicy tymczasowi świadczący pracę tymczasową na terenie Polski** na rzecz polskich pracodawców użytkowników,
- zostać **zatrudnieni przez agencję jako pracownicy tymczasowi świadczący pracę tymczasową na terenie innego państwa członkowskiego** na rzecz zagranicznych pracodawców użytkowników. W takim wypadku osoby te są delegowane do świadczenia pracy tymczasowej w innym państwie członkowskim (w trybie regulacji dotyczących unijnej swobody świadczenia usług),
- zostać **zatrudnieni przez pracodawców**, którzy jako kontrahenci danej agencji zatrudnienia zlecili jej wykonywanie czynności z zakresu legalizacji pobytu i zatrudnienia.

W każdym z tych przypadków, aby mogło dojść do zatrudnienia wspomnianych osób, a następnie ich delegowania, konieczne jest wykonanie przez agencję zatrudnienia szeregu czynności, np.:

- uzyskanie numeru PESEL we właściwym urzędzie miasta/gminy,
- dokonanie meldunku, przy okazji którego można uzyskać numer PESEL,
- uzyskanie certyfikatu rezydencji podatkowej we właściwym urzędzie skarbowym który jest niezbędny na potrzeby uzyskania dokumentu A1,
- uzyskanie pozwolenia na pracę/dokonanie rejestracji oświadczenia o powierzeniu wykonywania pracy cudzoziemcowi,
- uzyskanie właściwej wizy warunkującej otrzymanie dokumentu A1,
- wypełnienie formularza US – 54,
- dokonanie odpowiednich opłat administracyjnych (np. tytułem uzyskania pozwolenia na pracę).

Podkreślenia wymaga fakt, że w praktyce w przypadku cudzoziemców niejednokrotnie organy administracji publicznej wymagają przekazania im znacznie więcej danych, niż w przypadku obywateli Polski. Przykładem jest procedura ZUS związana z uzyskaniem dokumentu A1, w trakcie której wymagane są dane dot. sytuacji rodzinnej, życiowej itp.

Role podmiotów przetwarzających dane osobowe

Z punktu widzenia formalnego, szereg czynności legalizacyjnych może być samodzielnie wykonany przez cudzoziemca. Praktyka wskazuje jednak, że jest to utrudnione choćby z uwagi na barierę językową oraz brak znajomości przepisów i procedur.

Z tych względów niemalże regułą jest, że agencja zatrudnienia działa w imieniu cudzoziemca i samodzielnie dopełnia większości formalności związanych z legalizacją jego pobytu i zatrudnienia.

Należy przyjąć, że w przypadkach, gdy agencja zatrudnia cudzoziemca, dla którego uprzednio realizowała czynności z zakresu legalizacji, działa jako administrator jego danych osobowych. Z kolei w przypadku, gdy agencja działa na zlecenie swojego kontrahenta, który po zakończeniu procedury legalizacji zatrudnia cudzoziemca, wówczas działa jako procesor.

Biorąc pod uwagę fakt, że większość czynności realizowanych jest na etapie poprzedzającym zatrudnienie danego cudzoziemca, jako podstawę przetwarzania danych osobowych w procesie legalizacji pobytu i zatrudnienia można wskazać:

- żądanie danego cudzoziemca podjęcia przez agencję zatrudnienia określonych działań **przed zawarciem umowy** (art. 6 ust. 1 lit. b RODO), np. prośba cudzoziemca o dokonanie w jego imieniu meldunku czy uzyskanie certyfikatu rezydencji podatkowej,
- **wypełnienie obowiązku prawnego** spoczywającego na administratorze (art. 6 ust. 1 lit. c RODO), np. rejestracja we właściwym urzędzie oświadczenia o powierzeniu wykonywania pracy cudzoziemcowi,
- **zgodę** cudzoziemca na przetwarzanie danych osobowych (art. 6 ust. 1lit. a RODO).

Z uwagi na fakt, że proces legalizacji pobytu i zatrudnienia jest wieloetapowy i składa się z szeregu czynności, w praktyce wszystkie ze wspomnianych podstaw przetwarzania danych osobowych znajdują w nim zastosowanie.

Pomimo, że zgoda cudzoziemca nie wydaje się być niezbędna, to jednak warto ją pozyskać, tym bardziej, że w wielu przypadkach niezbędne jest pozyskanie od niego pełnomocnictwa do działania przed właściwymi instytucjami. Warto w takim wypadku w ramach jednego dokumentu **połączyć wspomniane pełnomocnictwo oraz zgodę na przetwarzanie danych osobowych**. W treści zgody jako cel przetwarzania należy wskazać podejmowanie niezbędnych czynności związanych z legalizacją pobytu i zatrudnienia.

Oczywiście jak w każdym innym przypadku, również w przypadku legalizacji należy w stosunku do cudzoziemca spełnić obowiązek informacyjny, w wskazać w nim w szczególności kategorie odbiorców danych osobowych (tj. właściwe organy administracji publicznej).

Pochodzenie danych osobowych

W praktyce wielokrotnie zdarza się, że cudzoziemcy nie są rekrutowani samodzielnie przez agencje zatrudnienia, a „przekazywani" im przez zagranicznych pośredników. W tym kontekście należy pamiętać o wymogu wskazania źródła pochodzenia danych osobowych.

Podczas działań zmierzających do legalizacji pobytu i zatrudnienia nie można wykluczyć sytuacji, w ramach której agencja zatrudnienia będzie działała w imieniu swojego klienta, a przedmiotem świadczonej przez nią usługi będzie np. wyłącznie przygotowanie (wypełnienie) właściwych dokumentów legalizacyjnych czy też reprezentowanie klienta w toku właściwego postępowania legalizującego pracę na terenie Polski, podczas gdy podmiotem zatrudniającym tego cudzoziemca będzie sam klient. W takim wypadku należy przyjąć, że jakkolwiek agencja jest w posiadaniu danych osobowych cudzoziemca, którego dotyczy dane postępowanie, to jednak **działa w charakterze podmiotu przetwarzającego**. Występuje bowiem w imieniu swojego klienta, który wskazuje cele przetwarzania powierzonych jej danych osobowych. W takim wypadku konieczne jest zawarcie z klientem **umowy o powierzeniu przetwarzania danych osobowych**.

Po zakończeniu etapu związanego z legalizacją (lub czasem w jego trakcie) dochodzi do zatrudnienia cudzoziemca. Wówczas agencja zatrudnienia w dalszym ciągu występuje w roli administratora jego danych osobowych, z tym że już jako podmiot zatrudniający.

W aspekcie danych osobowych procedura delegowania obywateli państw trzecich zasadniczo nie różni się od delegowania obywateli Polski, z tym jednak zastrzeżeniem, że w toku niektórych procedur właściwe instytucje wymagają udostępnienia im szerszego zakresu danych osobowych (np. wspomniana procedura otrzymania dokumentu A1).

Obowiązki administratora danych

6

OBOWIĄZKI ADMINISTRATORA DANYCH

Przypomnienie zasad ogólnych

Administrator danych osobowych podczas ich przetwarzania zobowiązany jest do:

- zapewnienia odpowiednich środków organizacyjnych i technicznych, adekwatnych do stopnia ryzyka określonego na podstawie przeprowadzonej oceny skutków dla ochrony danych,
- zapewnienia, aby podmiot przetwarzający dane w jego imieniu efektywnie stosował wszystkie wskazane przez administratora środki organizacyjne i techniczne,
- przestrzegania zasad opisanych w Rozdziale III (PODSTAWOWE ZASADY PRZETWARZANIA DANYCH),
- terminowej realizacji żądań podmiotów danych omówionych w Rozdziale IV (PRAWA OSÓB, KTÓRYCH DANE DOTYCZĄ).

Prowadzenie rejestru czynności – art. 30 ust. 1 RODO

Administrator i jego przedstawiciel (podmiot przetwarzający dane w imieniu administratora na podstawie umowy powierzenia przetwarzania danych osobowych) mają obowiązek prowadzenia rejestru czynności przetwarzania danych osobowych, za które ponoszą odpowiedzialność.

Rejestr prowadzony jest w formie pisemnej, w tym elektronicznej. Ma charakter dokumentu wewnętrznego, ale jest udostępniany na żądanie organu nadzorczego w celu monitorowania prowadzonego przetwarzania.

Obowiązek prowadzenia rejestru **nie ma zastosowania** wobec administratora oraz podmiotu przetwarzającego zatrudniającego mniej niż 250 osób, chyba że czynności przetwarzania, które wykonuje:

- mogą powodować ryzyko naruszenia praw lub wolności osób, których dane dotyczą,
- nie mają charakteru sporadycznego lub obejmują szczególne kategorie danych osobowych, o których mowa w art. 9 ust. 1 RODO, lub
- dotyczą wyroków skazujących i czynów zabronionych, o czym mowa w art. 10 RODO.

Przykładowy szablon rejestru czynności przetwarzania dostępny jest na stronie Urzędu Ochrony Danych Osobowych dostępnej pod adresem: www.uodo.gov.pl.

Wyznaczenie inspektora danych osobowych (IOD) – art. 37 RODO

RODO określa w sposób generalny, którzy administratorzy są zobowiązani wyznaczyć Inspektora Ochrony danych – dalej „IOD". Administrator danych powinien powołać taką osobę w poniższych sytuacjach:

- gdy przetwarzania dokonuje organ lub podmiot publiczny, z wyjątkiem sądów w zakresie sprawowania przez nie wymiaru sprawiedliwości,
- gdy główna działalność administratora lub podmiotu przetwarzającego polega na operacjach przetwarzania, które ze względu na swój charakter, zakres lub cele wymagają regularnego i systematycznego monitorowania osób, których dane dotyczą na dużą skalę,
- gdy główna działalność administratora lub podmiotu przetwarzającego polega na przetwarzaniu na dużą skalę szczególnych kategorii danych osobowych lub danych osobowych dotyczących wyroków skazujących i czynów zabronionych.

We wszelkich pozostałych przypadkach, poza wyżej wymienionymi, administrator powinien rozważyć powołanie takiej funkcji, biorąc pod uwagę kontekst przetwarzania oraz jego znaczenie w swojej wiodącej działalności.

W agencjach zatrudnienia rekomenduje się powołanie IOD. Dla agencji zatrudnienia największe znaczenie ma rodzaj działalności , która polega na regularnym przetwarzaniu danych osobowych na dużą skalę. Jest to istota działalności agencji, a nie jej poboczna aktywność.

Co może być wyznacznikiem dużej skali działalności?

- liczba osób, których dane dotyczą,
- zakres przetwarzanych danych,
- czas, przez jaki dane są przetwarzane,
- zakres geograficzny przetwarzania danych.

Rekomendujemy też, aby organizacje, które nie powołały wewnętrznego IOD ani nie wykupiły zewnętrznej usługi w tym zakresie, utrzymywały kontakt z zewnętrznym ekspertem-specjalistą w zakresie ochrony danych osobowych. Osoba taka może zapewnić wsparcie oraz konsultacje np. w kwestiach zgłaszania naruszeń czy komunikacji z Prezesem Urzędu Ochrony Danych Osobowych.

IOD może być zarówno osoba z wewnątrz, jak i spoza organizacji, a także podmiot świadczący usługę. Jedna osoba albo podmiot może pełnić funkcję IOD dla grupy przedsiębiorstw np. grupy kapitałowej. Istotne jest, aby IOD był „łatwo dostępny" dla osób wewnątrz organizacji, które podejmują decyzje oraz działania związane z przetwarzaniem danych osobowych. Wynika to z jego obowiązków, do których należą m.in.:

- informowanie administratora, podmiotu przetwarzającego oraz pracowników, którzy przetwarzają dane osobowe, o obowiązkach spoczywających na nich na mocy rozporządzenia,
- monitorowanie zgodności procesu przetwarzania z RODO,
- współpraca z organem nadzorczym.

IOD powinien posiadać odpowiedni poziom wiedzy na temat prawa i praktyk w dziedzinie ochrony danych osobowych, w tym dogłębną znajomość przepisów RODO nt. operacji przetwarzania danych, jak i zabezpieczeń stosowanych u administratora.

W ramach wypełniania zadań IOD nie może otrzymywać instrukcji dotyczących sposobu rozpoznania sprawy, środków jakie mają zostać podjęte, czy celu jaki powinien zostać osiągnięty. Nie może zostać zobligowany do przyjęcia określonego stanowiska w sprawie z zakresu ochrony danych. Powinien mieć zapewnioną niezależność. Członkowie zarządu administratora danych, dyrektorzy działów IT, czy działów operacyjnych nie mogą sprawować funkcji IOD, ponieważ rodzi to konflikt interesów.

Obowiązkiem administratora lub podmiotu przetwarzającego jest opublikowanie danych kontaktowych IOD (adres e-mail lub numer telefonu kontaktowego), w tym również na stronie www, o ile taką prowadzi, oraz zawiadomienie właściwego organu nadzorczego o danych kontaktowych IOD.

Agencja, która wyznaczyła inspektora, zawiadamia o tym organ nadzorczy w terminie 14 dni od dnia jego wyznaczenia. Zasady dokonania tego zgłoszenia określa art. 10 ustawy o ochronie danych osobowych.

Warto dodać, że jeśli organizacja podejmie decyzję o niepowoływaniu IOD, należy taką decyzję udokumentować i uzasadnić. Należy pamiętać, że przetwarzanie danych w działalności agencji zatrudnienia to proces ciągły i zapewnienie zgodności z przepisami RODO i innymi przepisami o ochronie danych osobowych musi być dokonywane nieprzerwanie.

Zgłaszanie incydentów
Zgodnie z art. 33 RODO przewidziane są dwa rodzaje incydentów (zgłoszenia naruszeń ochrony danych osobowych):

- zgłoszenie przez administratora organowi nadzorczemu zaistnienia incydentu (art. 33 ust. 1 RODO),
- zgłoszenie przez podmiot przetwarzający administratorowi zaistnienia incydentu (art. 33 ust. 2 RODO).

Zgodnie z art. 4 pkt 12 RODO poprzez naruszenie ochrony danych osobowych rozumie się naruszenie bezpieczeństwa prowadzące do przypadkowego lub niezgodnego z prawem zniszczenia, utracenia, zmodyfikowania, nieuprawnionego ujawnienia lub nieuprawnionego dostępu do danych osobowych przesyłanych, przechowywanych lub w inny sposób przetwarzanych.

W przypadku naruszenia ochrony danych osobowych administrator bez zbędnej zwłoki, jednak **nie później niż w terminie 72 godzin** od stwierdzenia naruszenia, ma obowiązek zgłosić je organowi nadzorczemu, chyba że jest mało prawdopodobne, by naruszenie to skutkowało ryzykiem naruszenia praw lub wolności osób fizycznych. W tym miejscu warto zwrócić uwagę, iż zgłoszenie może być sukcesywnie uzupełniane w toku podjętych działań, jeżeli administrator uzyskał dodatkowe informacje. Kluczowe wydaje się, by we wskazanym powyżej terminie, poinformować organ o zaistniałym zdarzeniu, nawet jeżeli nie posiadamy pełnego obrazu sytuacji i kompletu informacji.

Do zgłoszenia przekazanego organowi nadzorczemu po upływie 72 godzin dołącza się wyjaśnienie przyczyn opóźnienia.

Rekomendujemy, aby do zgłoszenia naruszenia ochrony danych osobowych do organu nadzorczego wykorzystywać formularz udostępniony przez PUODO na stronie https://uodo.gov.pl/.

Administrator jest zobowiązany do dokumentowania wszelkich naruszeń ochrony danych osobowych, w tym okoliczności naruszenia ochrony danych osobowych, jego skutków oraz podjętych działań zaradczych.

Więcej informacji na temat obowiązków administratora danych osobowych związanych z naruszeniami można znaleźć w dedykowanym poradniku umieszczonym na stronie PUODO – https://uodo.gov.pl/. Zawiera on również istotne sugestie ze strony

organu nadzorczego w zakresie sposobu oraz informacji, jakich należy udzielić podczas powiadamiania podmiotów danych o zaistniałym zdarzeniu.

Ważne:
Jeżeli administrator nie zawiadomi osób, których dane zostały naruszone, zawiadomi je zbyt późno lub w niewłaściwy sposób, może to rodzić wiele negatywnych konsekwencji. Oprócz strat wizerunkowych, należy wskazać tutaj ryzyko wszczęcia postępowania administracyjnego przez PUODO, które może zakończyć się nakazem zawiadomienia osoby, której dane dotyczą, o naruszeniu ochrony danych osobowych w celu przekazania jej wszystkich informacji wymaganych zgodnie z art. 34 ust. 2 RODO bądź też wydaniem ostrzeżenia, udzieleniem upomnienia, jak również nałożeniem przez organ nadzorczy kary administracyjnej.

Zawiadamianie osoby, której dane dotyczą, o naruszeniu

Jeżeli naruszenie ochrony danych osobowych spowodowało wysokie ryzyko naruszenia praw lub wolności osób fizycznych, administrator musi również zawiadomić osoby, których dane dotyczą. Odstąpić od tego obowiązku można wyłącznie w sytuacjach wskazanych w przepisach, tj.:

- gdy administrator wdrożył odpowiednie techniczne i organizacyjne środki ochrony i środki te zostały zastosowane do danych osobowych, których dotyczy naruszenie, np. poprzez zaszyfrowanie danych w sposób zapewniający ich bezpieczeństwo,
- gdy administrator zastosował następnie środki eliminujące prawdopodobieństwo wysokiego ryzyka naruszenia praw lub wolności osoby, której dane dotyczą,
- gdy takie zawiadomienie wymagałoby niewspółmiernie dużego wysiłku (co należy z pewnością ustalać przy uwzględnieniu kosztu zawiadomienia oraz potencjalnych strat związanych z jego brakiem), jednakże w takim przypadku administrator musi wydać publiczny komunikat (np. na stronie internetowej) lub zastosować podobny środek tak, aby osoby, których dane zostały ujawnione, zostały poinformowane o naruszeniu w równie skuteczny sposób.

Warto dodać, że według poradnika UODO „Obowiązki administratorów danych związane z naruszeniami ochrony danych osobowych", opublikowanego w maju 2019 roku, znacząca większość przypadków naruszeń dotyczących numeru PESEL powoduje wysokie ryzyko naruszenia praw i wolności osób fizycznych i musi być zgłaszana do organu nadzorczego.

Sankcje

7

SANKCJE

W przypadku stwierdzenia naruszenia przepisów RODO, organ nadzorczy ma prawo nałożyć na administratora lub podmiot przetwarzający **kary pieniężne** (art. 83 RODO).

Naruszenie przepisów dotyczących m.in. obowiązków administratora i podmiotu przetwarzającego w zakresie stosowania zasady ochrony danych w fazie projektowania, domyślnej ochrony danych, notyfikacji naruszeń, prowadzenia rejestru czynności przetwarzania czy niewyznaczenia inspektora ochrony danych wbrew takiemu obowiązkowi podlegają administracyjnej karze pieniężnej w wysokości do **10 000 000 EUR**, a w przypadku przedsiębiorstw do **2% całkowitego rocznego światowego obrotu** z poprzedniego roku obrotowego, przy czym zastosowanie ma kwota wyższa.

Naruszenie przepisów dotyczących m.in. podstawowych zasad przetwarzania danych osobowych, warunków uzyskania zgody, czy niezgodnym z przepisami przekazaniem danych do państwa trzeciego podlegają administracyjnej karze pieniężnej w wysokości do **20 000 000 EUR**, a w przypadku przedsiębiorstw **do 4% całkowitego rocznego światowego obrotu** z poprzedniego roku obrotowego, przy czym zastosowanie ma kwota wyższa.

Przy ustalaniu wysokości kary pieniężnej organ zwraca m. in. uwagę na:

- charakter, wagę i czas trwania naruszenia,
- umyślny lub nieumyślny charakter naruszenia,
- działania podjęte w celu zminimalizowania szkody,
- sposób, w jaki organ dowiedział się o naruszeniu,
- stosowanie zatwierdzonych kodeksów postępowania.

Warto pamiętać, o tym że organowi nadzorczemu przysługuje, obok wachlarza kar administracyjnych, szereg innych uprawnień określonych w art. 58 ust. 2 RODO. Na ich podstawie Prezes UODO może:

- wydawać ostrzeżenia dotyczące możliwości

naruszenia RODO,
- udzielać upomnień w przypadku naruszenia RODO,
- nakazać administratorowi lub podmiotowi przetwarzającemu spełnienie żądania osoby, której dane dotyczą,
- **wprowadzić czasowe lub całkowite ograniczenia przetwarzania, w tym zakaz przetwarzania**,
- nakazać administratorowi lub podmiotowi przetwarzającemu dostosowanie operacji przetwarzania do przepisów RODO, a w stosownych przypadkach wskazać sposób i termin na jego dostosowanie,
- nakazać administratorowi zawiadomienie osoby, której dane dotyczą, o naruszeniu ochrony danych,
- podjąć decyzję o cofnięciu certyfikacji lub nakazać podmiotowi certyfikującemu cofnięcie certyfikacji jak również zakazać jej udzielania,
- nakazać zawieszenia przepływu danych do odbiorcy w państwie trzecim lub do organizacji międzynarodowej.

Nałożenie administracyjnej kary pieniężnej lub wydanie ostrzeżenia nie wpływa na możliwość zastosowania przez Prezesa UODO innych uprawnień, czy sankcji. W toku jednego postępowania PUODO może jednocześnie zastosować wobec administratora danych upomnienie bądź zastosować ostrzeżenie, zaś w konsekwencji nierespektowania w dalszym ciągu przepisów z zakresu ochrony danych, na administratora może zostać nałożona kara pieniężna.

Wykaz dokumentów w zakresie RODO występujących najczęściej w agencjach zatrudnienia

8

WYKAZ DOKUMENTÓW W ZAKRESIE RODO WYSTĘPUJĄCYCH NAJCZĘŚCIEJ W AGENCJACH ZATRUDNIENIA (wraz z niektórymi wzorami[7])

Klauzule zgody na przetwarzanie danych osobowych:

ZGODA 1 – WZÓR

Wyrażam zgodę na przetwarzanie przez ..... (nazwa firmy) z siedzibą w ..... (adres firmy) podanych przeze mnie danych osobowych zawartych w cv i innych dokumentach związanych z rekrutacją, dla celów prowadzenia rekrutacji, w której biorę udział, w tym na udostępnienie podanych przeze mnie danych osobowych podmiotom, na rzecz których prowadzona jest rekrutacja/odbiorców świadczonych przez administratora usług, w świadczeniu których będę brała/brał udział. Oświadczam, że administrator danych osobowych spełnił w stosunku do mnie obowiązek informacyjny wynikający z przepisów prawa.

.....
podpis, data

ZGODA 2 (na przyszłe procesy) – WZÓR

Wyrażam zgodę na przetwarzanie podanych przeze mnie danych osobowych przez ..... (nazwa firmy) z siedzibą w ..... (adres firmy), dla celów prowadzenia przyszłych rekrutacji, w tym na udostępnienie podanych przeze mnie danych osobowych podmiotom, na rzecz których rekrutacje te będą prowadzone/odbiorców świadczonych przez administratora usług, w świadczeniu których będę brała/brał udział. Oświadczam, że administrator danych osobowych spełnił w stosunku do mnie obowiązek informacyjny wynikający z przepisów prawa.

.....
podpis, data

7 Wzory należy dostosować według własnych potrzeb biznesowych

Klauzule informacyjne dotyczące przetwarzania danych osobowych:
Uwaga wstępna: Zaleca się, aby klauzula informacyjna dotycząca przetwarzania danych osobowych w formie cyfrowej (w odróżnieniu od papierowej) była podana w sposób warstwowy. Treść pierwszej warstwy, zawierającej podstawowe informacje o przetwarzaniu, powinna być wyświetlana łącznie z treścią zgód (na tym samym ekranie). Te podstawowe informacje powinny wskazywać: tożsamość administratora danych, cel przetwarzania danych oraz opis praw osoby, której dane dotyczą. Ponadto z informacji podanej w pierwszej warstwie powinno jasno wynikać, jakie są konsekwencje przetwarzania danych (np. niewyrażenie zgody na przetwarzanie danych skutkuje brakiem możliwości wzięcia udziału w procesie rekrutacyjnym). Kolejna warstwa informacji powinna być możliwa do odnalezienia i wyświetlenia w prosty sposób. Nie można zmuszać osoby udzielającej zgód do aktywnego poszukiwania informacji znajdujących się w kolejnych warstwach klauzuli. Drugą warstwę informacji może stanowić link (kod QR) do polityki prywatności.

REKRUTACJA PRACOWNIKÓW – WZÓR KLAUZULI INFORMACYJNEJ

Informujemy, że administratorem Pani/Pana danych osobowych jest ..... (nazwa, adres siedziby). Udostępnione przez Panią/Pana dane osobowe przetwarzane są dla celów udziału w procesie rekrutacji na stanowisko, na które Pani/Pan aplikuje, a w przypadku wyrażenia przez Panią/Pana osobnej zgody, również dla celów przyszłych rekrutacji.

Podstawę prawną przetwarzania danych osobowych stanowi Pani/Pana zgoda, jak również właściwe przepisy prawa.

Zgoda może być w każdej chwili cofnięta, przy czym jej cofnięcie pozostaje bez wpływu na zgodność z prawem przetwarzania, którego dokonano na jej podstawie. Cofnięcie zgody powoduje, że Pani/Pana udział w procesie rekrutacji nie będzie możliwy.

Odbiorcami Pani/Pana danych osobowych są: podmioty przetwarzające dane w jego imieniu;

podmioty współpracujące (w tym kontrahenci, na rzecz których prowadzone są procesy rekrutacji); organy administracji publicznej, przy zachowaniu wymogów określonych obowiązującymi przepisami, w tym wymogu poufności oraz w zakresie niezbędnym do dokonania danej czynności.

Dane osobowe przetwarzane są przez czas trwania procesu rekrutacji, w którym bierze Pani/Pan udział, a w przypadku wyrażenia przez Panią/Pana osobnej zgody, również przez czas trwania przyszłych rekrutacji, jednak nie dłużej niż ..... lat/miesięcy. Czas ten może być skrócony w przypadku wycofania udzielonej przez Panią/Pana zgody.

Przysługuje Pani/Panu prawo żądania: dostępu do swoich danych osobowych, ich usunięcia, przenoszenia, sprostowania, ograniczenia przetwarzania, jak również prawo do wniesienia skargi do właściwego organu nadzorczego.

Podanie danych osobowych jest wymogiem umownym i ustawowym. Podanie danych osobowych jest dobrowolne, niemniej stanowi warunek Pani/Pana udziału w procesie rekrutacji.

Kontakt do Inspektora Ochrony Danych .....

.....

potwierdzenie zapoznania się, podpis kandydata, data

Uwaga: w ocenie autorów, aby w treści klauzul informacyjnych wspominać o transferze danych osobowych do państw trzecich oraz o profilowaniu jedynie wówczas, gdy wspomniany transfer oraz profilowanie mają miejsce.

PRACA TYMCZASOWA – WZÓR KLAUZULI INFORMACYJNEJ

Informujemy, że administratorem danych osobowych osoby świadczącej pracę tymczasową jest ..... (nazwa, adres siedziby).

Przetwarzanie obejmuje udostępnione przez Panią/Pana dane osobowe niezbędne do realizacji stosunku pracy/umowy cywilnoprawnej w zakresie określonym obowiązującymi przepisami, w tym przepisami ustawy z dnia 26 czerwca 1974 roku Kodeks pracy, ustawy z dnia 23 kwietnia 1964 roku Kodeks cywilny oraz ustawy z dnia 9 lipca 2003 roku o zatrudnianiu pracowników tymczasowych.

Podstawę prawną przetwarzania Pani/Pana danych osobowych stanowi przepis prawa albo umowa o pracę tymczasową/umowa cywilnoprawna zawarta pomiędzy administratorem danych osobowych a osobą świadczącą pracę tymczasową, a w zakresie stosunku pracy również przepisy ustawy z dnia 26 czerwca 1974 Kodeks pracy (art. 221), konieczność realizacji przez administratora obowiązków wynikających z przepisów prawa, jak również zgoda.

Administrator przetwarza dane osobowe dla celów realizacji stosunku pracy/umowy cywilnoprawnej oraz na potrzeby wykonywania obowiązków określonych obowiązującymi przepisami, w tym przepisami prawa pracy, ubezpieczeń społecznych, prawa podatkowego.

Odbiorcami Pani/Pana danych osobowych są: podmioty przetwarzające dane w jego imieniu; podmioty współpracujące (w tym pracodawcy użytkownicy, na rzecz których świadczą Pani/Pan pracę tymczasową); organy administracji publicznej, przy zachowaniu wymogów określonych obowiązującymi przepisami, w tym wymogu poufności oraz w zakresie niezbędnym do dokonania danej czynności.

Pani/Pana dane osobowe przetwarzane są przez czas trwania stosunku pracy/umowy cywilnoprawnej, a po ich zakończeniu przez okres określony obowiązującymi przepisami, w tym w zakresie

przechowywania akt pracowniczych.

Przysługuje Pani/Panu prawo dostępu do swoich danych osobowych, ich sprostowania, ograniczenia przetwarzania, jak również prawo do wniesienia skargi do właściwego organu nadzorczego.

Podanie ww. danych osobowych jest wymogiem ustawowym określonym przez przepisy, w tym przepisy ustawy z ustawy z dnia 26 czerwca 1974 roku Kodeks pracy oraz przepisy ustawy z dnia 9 lipca 2003 roku o zatrudnianiu pracowników tymczasowych.

Kontakt do Inspektora Ochrony Danych .....

.....

potwierdzenie zapoznania się, podpis pracownika tymczasowego, data

Uwaga: w ocenie autorów, aby w treści klauzul informacyjnych wspominać o transferze danych osobowych do państw trzecich oraz o profilowaniu jedynie wówczas, gdy wspomniany transfer oraz profilowanie mają miejsce.

PRACOWNICY WEWNĘTRZNI – WZÓR KLAUZULI INFORMACYJNEJ

Informujemy, że administratorem danych osobowych pracownika jest ..... .

Dane kontaktowe inspektora ochrony danych osobowych: ..... .

Przetwarzanie obejmuje udostępnione przez Panią/Pana dane osobowe niezbędne do realizacji stosunku pracy w zakresie określonym obowiązującymi przepisami, w tym przepisami ustawy z dnia 26 czerwca 1974 roku Kodeks pracy.

Podstawę prawną przetwarzania Pani/Pana danych osobowych stanowi umowa o pracę zawartą pomiędzy administratorem danych osobowych (pracodawcą), a pracownikiem, przepisy ustawy z dnia 26 czerwca 1974 Kodeks pracy (art. 221), konieczność realizacji przez administratora obowiązków wynikających z przepisów prawa, jak również zgoda.

Administrator przetwarza dane osobowe dla celów realizacji stosunku pracy oraz na potrzeby wykonywania obowiązków określonych obowiązującymi przepisami, w tym przepisami prawa pracy, ubezpieczeń społecznych, prawa podatkowego.

Odbiorcami Pani/Pana danych osobowych są: podmioty przetwarzające dane w imieniu administratora; podmioty współpracujące; organy administracji publicznej, przy zachowaniu wymogów określonych obowiązującymi przepisami, w tym wymogu poufności oraz w zakresie niezbędnym do dokonania danej czynności.

Pani/Pana dane osobowe przetwarzane są przez czas trwania stosunku pracy, a po jego zakończeniu przez czas określony obowiązującymi przepisami, w tym w zakresie przechowywania akt pracowniczych.

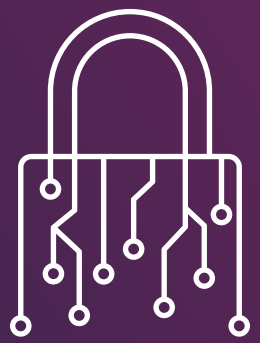
Przysługuje Pani/Panu prawo dostępu do swoich danych osobowych, ich sprostowania, ograniczenia

przetwarzania, jak również prawo do wniesienia skargi do właściwego organu nadzorczego.

Podanie ww. danych osobowych jest wymogiem ustawowym określonym przez przepisy, w tym przepisy ustawy z ustawy z dnia 26 czerwca 1974 roku Kodeks pracy.

Kontakt do Inspektora Ochrony Danych .....
.....
potwierdzenie zapoznania się, podpis pracownika, data

Uwaga: w ocenie autorów, aby w treści klauzul informacyjnych wspominać o transferze danych osobowych do państw trzecich oraz o profilowaniu jedynie wówczas, gdy wspomniany transfer oraz profilowanie mają miejsce.



Suplement:

Wybrane techniczne
i organizacyjne środki zabezpieczeń
danych osobowych

9

SUPLEMENT

WYBRANE TECHNICZNE I ORGANIZACYJNE ŚRODKI ZABEZPIECZEŃ DANYCH OSOBOWYCH

RODO bardzo oszczędnie wypowiada się co do środków i sposobów zabezpieczeń technicznych i organizacyjnych zalecanych do stosowania przy przetwarzaniu danych osobowych, wskazuje jedynie m.in. na pseudonimizację i anonimizację danych jako sposoby zabezpieczenia danych.

Stosowanie środków zabezpieczających powinno opierać się na analizie ryzyka, którą należy uaktualniać wraz ze zmianą procesów, systemów IT, czynników zewnętrznych czy przepisów prawa. W przygotowaniu analizy ryzyka może pomóc **norma PN-ISO 31000:2018 Zarządzanie ryzykiem – Wytyczne**.

Stosowanie zasady ochrony danych **w fazie projektowania oraz zasady domyślnej ochrony danych** przyczynia się do minimalizacji zidentyfikowanych ryzyk. W ramach tych dwóch zasad można zastosować poniższe działania:

- minimalizację danych, czyli zbieranie wyłącznie danych niezbędnych dla realizacji procesów biznesowych, co może oznaczać gromadzenie danych od mniejszej grupy osób lub mniejszej liczby danych od wyznaczonej grupy,
- ukrywanie danych poprzez ograniczenie dostępu do danych, szyfrowanie danych czy ograniczenie połączeń między danymi,
- separację danych logiczną bądź fizyczną,
- abstrakcyjność danych, czyli agregację rekordów jednego rodzaju,
- informowanie, czyli dostarczenie podmiotom danych informacji zgodnie z RODO w formie jasnego i krótkiego komunikatu (także ikonografiki),
- kontrolowanie przepływu danych przez podmiot danych, czyli pozyskiwanie zgód, aktualizację danych oraz umożliwienie realizacji praw osób fizycznych,
- zarządzanie poprzez publikację polityk, procedur oraz weryfikację ich wdrożenia,
- demonstrowanie rozliczalności poprzez zachowywanie decyzji, prowadzenie audytów, kontroli

i przeglądów oraz sporządzanie raportów dla władz spółki czy organizacji[8].

W ramach **technicznych środków zabezpieczenia danych** należy rozważyć stosowanie m.in.:

- 2FA (także multifactor), czyli tzw. uwierzytelniania dwupoziomowego, które polega na uzyskaniu dodatkowej autoryzacji podczas logowania do konta, np. poprzez wprowadzenie kodu lub frazy otrzymanej na urządzenie przenośne,
- korzystanie z VPN (ang. virtual private network), czyli tuneli, przez które płynie ruch w ramach sieci prywatnej pomiędzy nadawcą a odbiorcą za pośrednictwem sieci publicznej (Internetu) podczas korzystania z zasobów informatycznych organizacji,
- korzystanie tylko z zabezpieczonych, domowych sieci wifi w przypadku pracy zdalnej lub z hotspotów utworzonych na telefonach służbowych (potrzebny jest dość duży pakiet transmisji danych np. 50 MB),
- zasady ograniczonego dostępu tylko dla osób, które są zaangażowane w dany proces przetwarzania danych osobowych (tzw. dostęp na zasadzie need-to-know) z minimalnymi uprawnieniami umożliwiającymi im efektywną realizację zadań,
- stosowanie długich haseł dostępu do kont, zawierających co najmniej 16 znaków, oraz mechanizmu wymuszającego okresową ich zmianę,
- monitoring dostępu do danych np. poprzez analizę logów lub zastosowanie rozwiązań typu SIEM (ang. Security Information and Event Management),
- rozwiązań typu Data Loss Protection (DLP), które pozwalają na monitorowanie np. załączników w poczcie e-mail, a także na ostrzeganie użytkowników w zdefiniowanych wcześniej sytuacjach lub blokowanie zachowań (np. przy próbie wysłania na zewnątrz plików zawierających dane osobowe, czy eksporcie z systemu całej bazy danych osobowych do pliku),
- szyfrowania dysków twardych urządzeń przenośnych, rozwiązań typu MDM (ang. Mobile Device Management) umożliwiających m.in. zdalną konfigurację tych urządzeń, ich blokadę czy usunięcie danych,
- uwzględnienia bezpieczeństwa informacji w fazie projektowania aplikacji poprzez określenie wymagań „niefunkcjonalnych" z zakresu

8 Według „A Guide to Privacy by Design" opublikowanego przez Agencia Española de Protección de Datos 5.10.2019.

bezpieczeństwa zgodnych z uznanymi najlepszymi praktykami (np. OWASP TOP 10),
- regularnych testów penetracyjnych aplikacji i systemów wystawionych do Internetu, aby w porę wykryć i załatać luki w bezpieczeństwie tych aplikacji,
- zabezpieczeń biur i miejsc przetwarzania danych osobowych poprzez np. elektroniczne karty dostępu,
- używanie filtrów na ekrany komputerów przy pracy w miejscach publicznych czy podczas podróży służbowych,
- anonimizację danych, co do których wygasł czas retencji,
- pseudonimizację danych pozostających w użytku i szyfrowanie baz danych.

Organizacyjne środki ochrony danych to m.in:
- powołanie wykwalifikowanego Inspektora Ochrony Danych z wiedzą w zakresie przepisów prawa dotyczących ochrony danych osobowych oraz wiedzą techniczną na temat możliwych do zastosowania zabezpieczeń systemów i sieci,
- szkolenia, webinaria, akcje informacyjne, komunikaty, ulotki i wszelkie inne formy komunikacji w ramach podnoszenia świadomości użytkowników (tzw. security awareness),
- wydanie upoważnień do przetwarzania danych osobowych oraz zobowiązań do zachowania poufności dla osób mających dostęp do danych osobowych,
- podpisanie stosownych umów powierzenia z procesorami, którzy przetwarzają dane osobowe w imieniu administratora danych,
- weryfikacja przyszłych i obecnych procesorów poprzez formularze samooceny (self-assessment) oraz przeprowadzanie audytów zdalnych i na miejscu u procesorów,
- wprowadzenie polityk, procedur i instrukcji związanych z przetwarzaniem danych osobowych oraz regularna weryfikacja ich stosowania.

Stosowanie środków bezpieczeństwa powinno być poprzedzone analizą zakresu, kontekstu i celów przetwarzania danych osobowych oraz analizą ryzyka, zaś zastosowane środki techniczne i organizacyjne muszą być adekwatne do zapewnienia ochrony na właściwym poziomie. W określeniu potrzeb organizacji mogą pomóc normy PN-EN ISO/IEC 27001: 2017 i PN-EN ISO/IEC 27002:2017, a także norma PN-EN ISO/IEC 27701:2019.

Polskie Forum HR

www.polskieforumhr.pl

Polskie Forum HR jest najbardziej wpływową organizacją pracodawców reprezentującą rynek agencji zatrudnienia. Od 2002 roku działa na rzecz budowy efektywnego rynku pracy poprzez wpieranie zrównoważonego rozwoju usług w zakresie szeroko rozumianego doradztwa personalnego. Jest uznanym partnerem społecznym w Polsce i Europie.

Firmy członkowskie Polskiego Forum HR zatrudniają ponad **2,5 tys.** pracowników wewnętrznych w ponad 300 oddziałach na terenie całego kraju. W ubiegłym roku wsparły w zatrudnieniu blisko **300 tys.** osób zarówno w formie pracy tymczasowej, rekrutacji stałych, jak i delegowania za granicę.